IO-L’ESSERE

Il nodo centrale della speculazione jaspersiana intorno all’essere (sulla scorta dell’esperienza dell’equivocità e della multivocità dell’essere stesso) è quindi il tentativo di comprendere, o almeno di chiarire a livello esistenziale e indagare l’essere che non si risolve nel semplice svanire (cfr. PH, I 2; 111). Del resto, tanto l’essere che si risolve nello svanire oltre le determinazioni quanto quello che si lascia dire tutto mediante le categorie dell’intelletto non dicono nulla dell’essere che qui si indaga. E l’intero movimento della scienza, dal canto suo, altro non è che questo rifiuto dell’essere nello svanire e la ricerca dell’essere in sé.

Ora, sebbene da nessuna parte l’io abbia a che fare con l’essere chiuso in sé (cfr. PH, I 18; 130), proprio quell’essere nello svanire che è scartato dai costruttori del sapere scientifico è l’unico modo d’essere dell’essere per il pensiero. Lo svanire, quindi, è l’oggetto della ricerca filosofica che non vuole fermarsi all’oggetto (che, per definizione, non può essere l’essere). Del resto, dice Jaspers, ciò « che c’è è l’apparire non l’essere e neppure il nulla » (PH, I 19; 131) – anche se questo essere che c’è è tanto poco l’essere di cui l’io andava in cerca che pare quasi svanire nel nulla (cfr. PH, I 13; 124). Ora, la nullità di questo essere che c’è è però l’unico modo dell’essere: l’essere si dà per me sotto il segno della quasi nullità. Altrimenti detto, nel “divenire”. La dialettica hegeliana sembrerebbe rispettata, in questo punto, ma con uno slittamento che ne rivela, nell’interpretazione jaspersiana, il fondo esistenziale. O, meglio, è Jaspers che legge la dialettica essere-nulla- divenire nella sua valenza esistenziale. Nel divenire infatti (che è divenire temporale) l’essere che appare (fenomenologia dell’essere) porta con sé i

due precedenti (l'essere e il nulla), ma il prodotto, ossia il terzo, non è una nuova immediatezza come invece il terzo hegeliano. Esso infatti mantiene al suo interno quella forte lacerazione che l'ha generato, poiché in esso la duplicità rimane insuperabile: tanto l'essere-in-sé della trascendenza quanto l'essere nella coscienza per l'esistenza non sono l'essere, e in più non sono reciprocamente commensurabili (cfr. PH, I 20; 131).

La dialettica jaspersiana dell'essere si presenta quindi come una dialettica aperta in cui la memoria (Erinnerung) non è il medio della conciliazione degli opposti ma, al contrario, la traccia che l'io porta con sé dell'irriducibilità e dell'incommensurabilità degli opposti stessi. « Non c'è alcuna concezione dell'essere in grado di abbracciare tutto l'essere in cui ci troviamo. Questa è la mia situazione che, filosofando, non dimentico » (PH, I 22; 133 – corsivo mio).

Che ne è quindi dell'essere? Si chiede Jaspers (cfr. W, 37). È forse questo "diluirsi" dell'essere stesso in tutto ciò che indeterminatamente si può dire che è? O è la "fissazione" (starrwerden) del molteplice sensibile nell'essere categorialmente determinato che è conosciuto? O infine è quell'essere di cui mi posso accertare nel trascendimento di ogni oggettività mediante il pensiero? (cfr. PH, I 23; 135). In ogni caso, l'essere si presenta come una magna questio che non pare trovare una soluzione univoca: « l'essere, diviso dalle domande che lo riguardano non può essere riconosciuto nella sua unità » (PH, III 36; 972).

L'impossibilità di una risposta universalmente valida impone, in conformità con quanto precedentemente rilevato riguardo alla teoria dell'interpretazione, un ritorno sul domandante. Il fallimento della domanda apre la possibilità di una riflessione sul soggetto stesso della domanda. Non per una sorta di relativismo soggettivo di chi s'impone come misura di tutte le cose – di quelle che sono in quanto sono e di quelle che non sono in quanto non sono – ma per la necessità che

scaturisce dal fallimento stesso di ogni tentativo di determinazione univoca. L'essere non si dà quindi nella comprensione. Esso, in quanto abbracciante (Um-greifende) è di per sé in-comprensibile (Ungreifende). Ma l'in-comprensibilità dell'essere apre all'esistenza come unico ambito per una possibile risposta. Soggettiva forse, e quindi fallace o fallibile, ma una e non unica (cfr. PH, III, 416-417; 904-906), e comunque sempre possibile risposta sull'essere.

« A questo punto l'esistenza diventa il segno per indicare la direzione dell'auto-accertamento di un essere che non si può pensare oggettivamente, né in termini di universale validità; è l'essere che nessuno conosce e che nessuno può affermare nella pienezza del suo senso, né riferendosi a se stesso, né riferendosi ad altro » (PH, I 19; 130-131).

L'uomo è l'unica via d'accesso all'essere, in quanto è anche l'unico essere che è cosciente del proprio, pur inadeguato, essere. Non si danno altre possibilità. Del resto «L'eterogeneità dell'apparire (del fondo oggettivo nei fenomeni, della trascendenza dell'essere-in-sé nelle cifre, dell'esistenza nella certezza della coscienza assoluta) annulla in ogni sua direzione la consistente stabilità di un essere, perché nel suo complesso questa eterogeneità mantiene l'essere, a cui si rivolge la domanda dell'esistenza possibile nella realtà temporale, in una lacerazione definitiva che investe alla radice anche la domanda » (PH, I 21; 133).

La lacerazione (Zerrissenheit) dell'essere investe tutto l'essere e rimbalza sulla domanda stessa che, come detto, non trova una risposta univoca, ma segna anche il domandante che, in quanto tale, è anche l'unico interpellato. Il filosofare è quindi questo movimento del pensiero che ritorna sul soggetto il quale è chiamato a leggere e interpretare personalmente l'essere così come esso si presenta, ossia nell'apparire che come tale è nulla per il pensiero, ma che, come apparire dell'essere, è un qualcosa carico di significato (pur non essendo la verità): « il filosofare, attraverso l'apparire,

coglie l’essere nell’interpretazione delle cifre della trascendenza e nel pensiero che si appella all’esistenza » (PH, I 20; 132). L’essere quindi può essere scorto solo nel movimento riflessivo del pensiero che leggendo il fenomeno come cifra dell’essere (dalla fenomenologia dell’essere all’interpretazione delle cifre dell’essere stesso) non svela questo, riducendolo di volta in volta a un essere determinato e così perdendolo, come vorrebbe la conoscenza scientifica, ma si accerta di esso. L’interpretazione dell’essere è quindi sempre una, mai unica (ossia univoca e dogmatica). Ciò vuol dire che, trascendendone l’oggettività (che però in quanto tale è solo un prodotto o, kantianamente, una forma a priori del soggetto), il pensiero esperisce l’inadeguatezza dell’espressione categoriale, peraltro imprescindibile, e apre così all’accertamento dell’essere quale forma di conoscenza, ancora categoriale, ma non più oggettiva. Fare filosofia pare quindi voler dire, pascalianamente, beffarsi della filosofia. E tale inevitabile farsi beffe della filosofia, ironico e tragico allo stesso tempo, è il trascendere (cfr. PH, I 23; 134).

L’autentico essere, quindi, è da cercarsi solo nella trascendenza, o nel trascendimento. Non certo attraverso la coscienza in generale che indaga l’essere come un oggetto per un soggetto, ma tramite l’esistenza. Questo perché l’ontologia (ossia la dottrina dell’essere) può giungere solo a tradurre l’essere nei modi dell’essere stesso senza per questo poter mai comprendere l’essere come unico; al massimo essa può liberare il cammino per un ulteriore trascendimento. « Oggi l’ontologia non vale più come metafisica, ma come teoria delle categorie » (PH, I 24; 136). E ancora: « Qualunque cosa possa pensare il pensiero mi crea solo lo spazio dell’io come esistenza possibile che rimane sempre estranea al pensato » che, di per sé, ha solo « conoscibilità relativa », è « possibilità », « appello », nulla di più (PH, I 24; 136).

Ma come può una certezza chiarificatrice darsi in una

oggettivazione inadeguata? Del resto « l'essere, come essere-oggetto, non sussiste da sé », ma è solo un ens rationis (PH, I 30; 143). Questo sarà possibile solo se il soggetto è più e meno che soggetto: nonostante il soggetto, l'io è altro. Nel fallimento della soggettività del soggetto , l'io nella sua intenzionalità si rapporta a un essere non-oggettivo, e tale rapporto (ma è un rapporto impossibile!) è l'esistenza (PH, I 28; 140-141).

La prospettiva di una certezza fondata su di un impossibile rapporto al non-oggettivo non può che abbattere il pensiero categoriale (dell'intelletto) al pari dell'uomo che si limita a esserci senza svelare la sua natura intimamente sbilanciata verso la trascendenza (cfr. PH, I38, 152). Ma lo sconforto dell'esserci è al tempo stesso stimolo al trascendimento: « Nello sconforto dell'esserci c'è in me lo slancio dell'essere » (PH, II 204; 679). Il pensiero non è in grado di conoscere l'essere, ma solo di chiarire l'esistenza, quando si fa pensiero attivo nella vita stessa che attraverso il medio del linguaggio filosofico si traduce in appello. Appello a trascendere. « Tutte le sue vie conducono alla metafisica » (PH, I 32; 145).

«L'essere è rimasto in sospensione per l'incomprensibilità dell'essere-in-sé. Esso è apparso come un limite nell'analisi dell'esserci. Ma mentre l'essere-in-sé mi resta del tutto inaccessibile perché, come assoluta alterità, è quasi nulla per il pensiero, io sono a mia volta quell'io che è posto come limite all'analisi dell'esserci. Nella ricerca dell'esserci è questo il passo ulteriore che bisogna compiere » (PH, I 13; 124).

LA GERARCHIA

Anche Nietzsche ha il suo Socrate. Sono i pensatori liberi. Dicono: “Di cosa ti lamenti? Come sarebbe il trionfo dei deboli, se loro stessi non formassero una forza superiore?”

“Ci inchiniamo al fatto compiuto”: questo è il positivismo moderno: è destinato a portare avanti la critica dei valori, è inteso a respingere qualsiasi chiamata a valori trascendenti, che sono dichiarati fuori moda, ma solo nel ritrovarli, come forze che guidano il mondo attuale. Chiesa, morale, Stato, ecc.: Solo il loro valore viene discusso per ammirarne la forza e il contenuto umano.

Il libero pensatore ha la singolare abitudine di voler recuperare tutti i contenuti, tutto il positivo, ma senza mai interrogarsi sulla natura di questi contenuti che sono considerati positivi, né sull’origine né sulla qualità delle corrispondenti forze umane. È ciò che Nietzsche chiama “fatalismo”.

Il libero pensatore vuole recuperare il contenuto della religione, ma non chiede mai se la religione non contenga proprio le forze inferiori dell’uomo, che piuttosto dovrebbero desiderare di rimanere esterne. Ecco perché non è possibile fidarsi dell’ateismo di un libero pensatore, anche se è un democratico e un socialista: “La Chiesa ci disgusta ma il suo veleno no…”.

Questo è ciò che caratterizza principalmente il positivismo e l’umanesimo del libero pensatore: il “fatalismo”, l’incapacità di interpretare, l’ignoranza delle qualità della forza. Dal momento in cui qualcosa appare come una forza umana o come un fattore umano, il libero pensatore applaude, senza chiedersi se quella forza non è di bassa estrazione, e questo fatto è l’opposto di un fatto nobile: “Umano, troppo umano” .

Poiché non tiene conto delle qualità delle forze, il libero pensiero, per vocazione, è al servizio delle forze reattive e traduce il suo trionfo. Perché l'atto è sempre quello dei deboli contro i forti; "l'atto è sempre stupido, e mi è sempre sembrato più un bue che un dio."

Al libero pensatore Nietzsche oppone lo spirito libero, lo stesso spirito di interpretazione che giudica le forze dal punto di vista della loro origine e delle loro qualità: "Non ci sono fatti, solo interpretazioni".

La critica del libero pensiero è un tema fondamentale nel lavoro di Nietzsche. Senza dubbio perché questa critica scopre un punto di vista secondo cui diverse ideologie possono essere attaccate allo stesso tempo: positivismo, umanesimo, dialettica. Il gusto per l'atto nel positivismo, l'esaltazione del fattore umano nell'umanesimo, la mania di recuperare i contenuti umani nella dialettica.

La parola gerarchia ha due significati in Nietzsche. Significa, in primo luogo, la differenza tra le forze attive e reattive, la superiorità delle forze attive rispetto a quelle reattive. Nietzsche può quindi parlare di "un grado immutabile e innato nella gerarchia"; e il problema della gerarchia è lo stesso di quello degli spiriti liberi.

Ma la gerarchia indica anche il trionfo delle forze reattive, il contagio delle forze reattive e la complessa organizzazione che viene da esse, dove hanno vinto i deboli, dove i forti sono contaminati, dove lo schiavo che non ha cessato di essere uno schiavo prevale su un Signore che ha cessato di essere: il regno della legge e della virtù. E in questo secondo senso, la moralità e la religione sono ancora teorie della gerarchia.

Se si confrontano i due sensi, vedi che il secondo è come l'altra faccia del primo. Facciamo della Chiesa, della morale e dello Stato i signori o i detentori di ogni gerarchia.

Noi, che siamo essenzialmente reattivi, che prendiamo i

trionfi della reazione con una metamorfosi dell'azione, e gli schiavi dei nuovi padroni – noi, che non riconosciamo la gerarchia più del suo rovescio, abbiamo la gerarchia che meritiamo.

Nietzsche chiama schiavo il debole o non meno forte, ma a chi, a prescindere dalla sua forza, è separato da ciò che può. Il meno forte è forte quanto il forte se va fino alla fine, perché la beffa, la sottigliezza, la spiritualità e persino il fascino con cui completa la sua minima forza appartengono proprio a questa forza e non la rendono meno. La misurazione delle forze e la loro qualificazione non dipendono affatto dalla quantità assoluta ma dalla relativa realizzazione. Forza o debolezza non possono essere giudicate dal risultato della lotta e del successo.

Perché, ancora una volta, è un dato di fatto il trionfo del debole: è anche l'essenza del fatto. Si può solo giocarecon le forze tenendo conto, in primo luogo, della loro qualità, attiva o reattiva; secondo, l'affinità di questa qualità con il polo corrispondente della volontà di potenza, affermativa o negativa; in terzo luogo, la sfumatura della qualità che presenta la forza in questo o in un altro momento del suo sviluppo, in relazione alla sua affinità. Allora, la forza reattiva è:

1° la forza utilitaristica, adattamento e limitazione parziale;

2.º la forza che separa la forza attiva da ciò che può, che nega la forza attiva (trionfo dei deboli o degli schiavi);

3.º la forza separata da ciò che può, che nega se stessa o si rivolge contro se stessa (regno dei deboli o schiavi).

E, parallelamente, la forza attiva è:

l.º le forza plastiche dominano e soggiogano;

2.º la forza che va fino alla fine di ciò che può;

3.º la forza che afferma la sua differenza, che fa della differenza un oggetto di piacere e affermazione.

Le forze saranno determinate in modo concreto e completamente, solo se si tengono in conto, queste tre coppie di caratteri a loro volta.

TENEBRE CRUDELI

Sentimenti ineludibili mi circondano
Urla di ossessione
Guardo attraverso me
Una bestia è nata nel mio essere
Tenebre bestiali del profondo
Il male prende possesso
E libera lo spirito
Il lupo che vedo
È la bestia in me

Sono il Misantropo che calca il sentiero del cammino oscuro…

Il sangue è tutto attorno
Un bestia è nata nella mia anima …
Troppo breve è stato il momento
Sangue sulle mie mani
Questa è vendetta?
Un'ombra bestiale e profonda

Eclissi totale del cielo
La terra giace nelle ombre
Quando la luna splende in una luce fredda

Una battaglia contro i miei pensieri interiori

È come un taglio brutale nella mia anima
Soddisfa i miei sogni più profondi
Sensazione di liberazione totale
Posseduto da tutto ciò che è sconosciuto
Camminando attraverso la profondità interiore

Sono il Misantropo che calca il sentiero del cammino oscuro…

MISANTROPIA SENZA UMANITÀ

Ricevo e pubblico questa traduzione dell'affine "Annichilare", di un interessante disamina, che parte da un videogioco. È anche se non è una delle forme da Noi preferite, il testo da uno spaccato della Misantropia in particolare, che ribalta in termine in sé, è pone antagonisticamente – senza pero un dualismo concordante-la Tendenza Misantropica Antipolitica e Attiva, rispetto a quella passiva/politica…naturalmente perseguiamo incessantemente anche la formula perfetta: il "Tutto è Permesso", che ci permette di far espandere il Caos Misantropico abbattendo i ponti della morale umana…

In Inglese PDF da scaricare:

https://mega.nz/#!Tmo0gSJD!AslMyOoG3OChiMKYfD6s-NqW94t5HRTz-Sen9qub3Ww

https://web.archive.org/web/20190820134519/https://abissonichilista.altervista.org/misantropia-senza-umanita/

https://upload.disroot.org/r/eZ9RIUJb#BvRka7pfpVjPuTgSXW1+Y4LClN//Q8r6lsq1+aOVnTk=

_____

Le rappresentazioni sulla Misantropia sono spesso attribuite a una o entrambe le motivazioni. Il Misantropo è spesso rappresentato come dominato dalla passione o come guidato da un principio incessante. Il videogioco Plague Inc., che proietta i giocatori come un agente patogeno con l'obiettivo di annientare la specie umana, offre una Misantropia distinta. Ci invita e ci ingaggia nei valori di un virus, un batterio o un parassita, senza urti emotivi o fondamento logici, ci intrattiene nella possibilità di una Misantropia senza umanità.

La Misantropia è l'avversione o l'odio dell'umanità nel suo insieme. Il termine deriva dal greco μῖσος (odio) e ἄνθρωπος (umano). Le rappresentazioni della Misantropia, in letteratura e altrove, l'hanno spesso attribuita a una o entrambe i motivi. Da un lato, i Misantropi sono spesso raffigurati come governati dalla passione, dal loro intenso ed emotivo orrore per l'umanità, il risultato di affronti personali o avversità. Pertanto, il protagonista del Timon di Atene di Shakespeare (c.1605), sopraffatto dal risentimento e dal disprezzo per la società che ha aprofittato della sua generosità e buona volontà, si ritira nel deserto, desiderando solo di stare con gli affini; nelle righe finali dell'opera teatrale, l'epitaffio cataloga la speranza come "una piaga ti consumi, i malvagi codardi morti!" (V.4.71). D'altra parte, il Misantropo sarà guidato da un principio incessante, il cui disprezzo ragionato deriva da un codice morale di alta mentalità. In "Il Misantropo" di Molière (1666), l'insistenza intransigente di Alceste sull'onestà e sul parlare in parole, e il suo rifiuto di indulgere alle folle disoneste e agli sciocchi che lo circondano, porta allo stesso modo all'esilio auto-imposto: "Trovare su ogni ruolo di base, / L'ingiustizia, la frode, l'interesse personale, il tradimento. … / Ah, è troppo; l'umanità è finita così in basso, / intendo rompere con l'intera razza umana "(I.1). Timon è un eroe tragico, il

fumetto di Alceste, ma condividono il difetto del personaggio in eccesso: dove Timon è troppo generoso, Alceste è troppo onesto. Entrambi sono rappresentati come estremi, persino patologici, a modo loro, e la Misantropia viene posta come conseguenza fuorviante o sintomo di inclinazioni intemperanti.

Nel 2012 è stato prodotto un videogioco che offre ai giocatori l'opportunità di perseguire attivamente la maledizione di Timon sull'umanità. Plague Inc., sviluppata da Ndemic Creations per dispositivi mobili, ti proietta come agente patogeno: puoi scegliere tra batteri, virus, parassiti e una varietà di altri microrganismi. Giocato su una mappa del mondo, è necessario selezionare un paese in cui infettare il paziente zero e quindi vedere l'evolversi nel tempo manipolando tratti come la velocità e la modalità di trasmissione (in paesi aridi o umidi, ad esempio, o tramite corrieri come uccelli, insetti, roditori e bestiame), i sintomi che manifestano (tosse e starnuto. convulsioni, cisti e necrosi, tra molti altri) e la resistenza alle minacce ambientali e terapeutiche (climi estremi, antibiotici e così via).

L'obiettivo, che sembra difficile descrivere come qualcosa di diverso dalla Misantropia, è il diffondersi in tutto il mondo e cancellare la specie umana; i progressi vengono registrati per mezzo di continui racconti di coloro che si è riusciti a infettare e uccidere.

Col passare del tempo, si può approfittare delle opportunità per aumentare il contagio (migrazioni di massa di uccelli, raduni olimpici), ma, una volta che gli umani si sono resi conto di questo, si devono affrontare anche i tentativi di contenimento (confini chiusi, abbattimenti di animali) e la loro ricerca sempre più vigorosa per una cura. Il tempismo è cruciale: evolviti troppo velocemente e ucciderai i tuoi ospiti prima di poter infettare il mondo intero; oh troppo lento e si avrà tempo per sviluppare una cura. Il gioco è stato successivamente ampliato per includere scenari che

consentono di giocare con malattie specifiche, come la Morte Nera, il vaiolo e l'influenza suina, o in mondi alternativi, assaliti da un aumento del riscaldamento globale, crisi finanziarie o xenofobia, nonché con tipi di peste immaginaria completi come il worm Neurax, che prende il controllo delle menti dei suoi ospiti, e il virus Necroa, che trasforma gli infetti in zombi.

Nel 2014, Plague Inc. è stato ulteriormente ampliato, con una nuova malattia da collegare alla serie del film il "Pianeta delle scimmie"in nuove versioni . "L'Alba del Pianeta delle scimmie" (Wyatt 2011) racconta la storia dello sviluppo di un farmaco sperimentale a base virale che protegge e aumenta l'abilità cognitiva ma, sebbene stabile negli scimpanzé e in altre scimmie, si rivela fatale per l'uomo. Gli eventi portano alla fuga di un gruppo di scimmie potenziate dal virus mortale, e le scene di chiusura del film mostrano le scimmie che si ritirano in un rifugio nella foresta e l'infezione che si diffonde rapidamente in tutto il mondo. Con Plague Inc. nell'espansione "Simian Flu", che è stata prodotta in coincidenza con "L'Alba del Pianeta delle scimmie" (Reeves 2014), viene diffuso una volta in più un agente patogeno, ma questa volta ci sono due ceppi. È necessario sviluppare sia la variante umana, che è debilitante nei modi consueti, ma anche la forma della scimmia, che fa migliorare chi la ospita: il virus può aumentare la comunicazione, la coesione sociale, la comprensione del comportamento umano e altro ancora.

Si ottiene anche un certo controllo diretto sulle scimmie stesse e si è in grado di fondare colonie, spostare gruppi in tutto il mondo e salvare scimmie in cattività dai laboratori di ricerca. In effetti, si gioca allo stesso modo sia come scimmie, sia come virus, perseguendo obiettivi indipendenti ma complementari: fuga e distruzione dell'umanità.

Come viene rappresentata la Misantropia di Plague Inc. e l'espansione del Simian Flu? I giocatori sono incoraggiati a rifiutare l'umanità per passione o per principio o per

qualcos'altro? In effetti, nel corso del gioco non viene posta alcuna motivazione certa, per annientare la specie umana e i giocatori sono impegnati a perseguire il loro obiettivo raccapricciante senza urti emotivi o fondamento della logica. La fine dell'umanità è semplicemente l'obiettivo strategico del gioco e la qualità è il freddo calcolo astratto che pervade il gioco.

La grafica del gioco consiste principalmente nell'immagine satellitare semplificata del mondo, che mostra solo la topografia naturale di base punteggiata da icone per porti e aeroporti e una serie di diagrammi stilizzati dei vari tratti dell'agente patogeno; del tutto assenti sono rappresentazioni esplicite dell'intensa miseria e sofferenza e del devastante collasso sociale che sarebbe la realtà delle pandemie nei modelli di gioco. Le indicazioni degli effetti di una pestilenza vengono fornite solo sotto forma di grafici e tabelle che registrano il tasso di infezione o il numero di paesi colpiti, mediante comunicazioni e annunci concisi, minimamente informativi. Inoltre, il gioco non condanna o notifica in alcun modo il metodo in atto necessario per perseguire.

A differenza delle caratterizzazioni dei Misantropi Timon e Alceste, non ha senso nel videogioco che i cattivi desideri verso l'umanità siano impropri o fuorvianti o sintomatici di qualche aberrazione malsana. In Plague Inc., la Misantropia è patologica solo nel senso più letterale.

Il termine patologia si riferisce sia allo studio di "malattie e condizioni anatomiche e fisiologiche anormali", sia alle caratteristiche e al comportamento collettivi di tale condizione ("Patologia, N."). Per estensione colloquiale, qualcuno che è
patologico esibirà "una qualità o un tratto in una misura considerata estrema o psicologicamente malsana" ("Patologico, Adj. e N."), come Timon e Alceste. Il filosofo della scienza Georges Canguilhem sottolinea, tuttavia, che stabilire ciò che

conta come normale o patologico e la relazione tra questi due stati, non è affatto una questione semplice. Ciò che è normale non può semplicemente essere ciò che è più comune, come spesso si suppone: un individuo anomalo può essere perfettamente in salute e, in effetti, costituirà la propria norma, anche se non ha una media statistica (Canguilhem 144; Lechte 15). Inoltre, ogni particolare stato di un organismo, anche in uno stato patologico, sarà caratterizzato da modelli tipici di comportamento che sono appropriati per un organismo in quello stato, cioè sarà governato da norme (Gutting 47).

In effetti, Canguilhem sostiene: "Non esiste una patologia obiettiva. Strutture o comportamenti possono essere oggettivamente descritti ma non possono essere definiti "patologici" sulla base di alcuni criteri puramente oggettivi "(226). Accertare ciò che è normale o patologico non è una questione di applicazione di una regola assoluta, universale. Piuttosto, l'intera questione di ciò che è normale o patologico è altamente situata e dipende dalla natura dell'organismo specifico e dal suo ambiente. In particolare, dipende dall'esperienza vissuta di quell'organismo.

Una creatura vivente valuterà determinati stati rispetto ad altri: valorizzerà quelli che lo potenziano e gli consentiranno di prosperare su quelli che gielo impediscono o si adoperano per eliminarlo (Canguilhem 126–7; Gutting 47). "Gli esseri viventi preferiscono la salute alle malattie" (Canguilhem 222), e risolvere ciò che deve essere considerato normale o patologico sarà sempre una questione di tale preferenza e valutazione. Canguilhem ci ricorda, infatti, che è dal latino "valere", che significa essere in buona salute, che deriva il termine valore (201). Uno stato sano, sostiene in ultima analisi, non deve essere equiparato a una nozione astratta e generalizzata di ciò che è normale, ma è uno in cui un organismo, sia esso uccello, volpe o ameba, è in grado di tollerare le incostanze, gli incidenti di un ambiente e le infrazioni. È uno in cui una creatura è in grado di adattarsi

e uniformarsi a nuove situazioni e circostanze, vale a dire una in cui è in grado di funzionare secondo nuove norme, anzi di istituire nuove norme (Canguilhem 196–9; Gutting 47– 8).

Sembra esatto dire che Timon e Alceste manifestano qualità estreme che non sono salutari per loro e costituiscono, anche secondo l'attenta analisi di Canguilhem, una forma di patologia. Nessuno dei due è in grado di tollerare le incostanze, gli incidenti e le infrazioni con cui sono assediati, ed entrambi sono costretti a ritirarsi dalla società umana in maniera definitiva. Timon, infatti, non riesce completamente ad adattarsi alle nuove circostanze, questo con conseguenze fatali. Ciò che fa ammalare Timon e Alceste è l'incapacità dell'umanità di essere all'altezza delle proprie ampliate aspettative, di rispettare le norme che credono debbano valere per tutta la società civile.

In quanto tale, la loro frustrazione e furia è diretta verso coloro che riconoscono e apprendono come il loro stesso tipo: "quanto lontani / da razionali ci dispiace che queste creature siano così" dice Alceste (Molière V.7), e "La parvenza, sì te stesso, Timon disprezza questo "(Shakespeare IV.3.22). Il loro odio è, in verità, una forma di odio verso se stessi. Ed è in questo modo che queste rappresentazioni convenzionali della Misantropia ci hanno concesso che l'odio per l'umanità fosse patologico: cosa potrebbe essere più malsano che odiare se stesso?

È questo impulso autolesionista che alla fine è la deviazione o l'anomalia che determina la caduta dell'archetipo del Misantropo. Ma questa caratterizzazione della Misantropia come stato patologico è essa stessa, ovviamente, una valutazione, una rappresentazione particolare e pregiudizievole del Misantropo e l'oggetto della sua disaffezione. Nel considerare l'amore di sé di un individuo e il suo amore per l'umanità come equivalenti e necessari, esso definisce l'umanità stessa come la norma. In breve, è un ritratto antropocentrico di Misantropia o, meglio, quello che potremmo definire un

ritratto antroponormativo. Possiamo vederlo più chiaramente se osserviamo le circostanze in cui il termine Misantropia è effettivamente impiegato e quelle in cui non lo è.

Sebbene le definizioni di "Misantropia"nei dizionari, concentrandosi forse troppo da vicino sull'etimologia, ci dica semplicemente che è l'odio dell'umanità ("Misantropia, N."), la parola è stata infatti usata solo dagli umani che esprimono questo odio . La dannosa diatriba dell'agente Smith (Hugo Weaving) in "The Matrix" (Wachowski e Wachowski 1999), è alimentata da una repulsione viscerale dalla forma umana che gli è stato richiesto di adottare, è che spiega le ragioni della guerra delle macchine contro l'umanità: a differenza di tutte gli altri mammiferi, gli umani non regolano le loro interazioni con l'ambiente, ma si moltiplicano indefinitamente fino a quando non hanno consumato tutto ciò che li circonda, per poi diffondersi in un'altra area.

Gli esseri umani, afferma Smith, sono un virus o una malattia: "Sei una piaga e noi siamo la cura". Ma nonostante l'evidente passione e principio, sarebbe inappropriato descrivere l'agente Smith come un Misantropo. È una macchina e non c'è alcun elemento di auto-disgusto da deprecare. Allo stesso modo, in Plague Inc. né le varie malattie che lavorano per spazzare via l'umanità, né le scimmie potenziate che la evitano, possono essere giustamente definite Misantropiche, dato che si tratta di agenti disumani che non odiano se stessi.

Seguendo Canguilhem, ciò che rende patologici virus, parassiti, funghi, batteri e altri microrganismi è il fatto che hanno un impatto sull'esperienza vissuta di un particolare individuo umano. Tosse e starnuti, convulsioni e lesioni cutanee, ascessi e insufficienze degli organi, causate da una pestilenza impediranno, inabiliteranno e alla fine elimineranno questi individui. Una piaga è patologica perché viene valutata come tale da una prospettiva particolare, una prospettiva umana.

Ma l’agente Smith, la macchina, ha una valutazione completamente diversa di ciò che costituisce una piaga, e la cosiddetta Simian Flu in realtà migliora le scimmie che infetta. Plague Inc., con il suo gioco elaborato e calcolato, non è motivato né dalla passione né dai principi, pone soluzioni radicali alla prospettiva umana e istituisce norme disumane. Non si gioca come “umanità”, lottando per rimanere in salute di fronte a un ambiente mutevole e ostile, ma come la peste stessa, o come le scimmie, in costante evoluzione, trasformando se stessi per sconfiggere e superare il proprio avversario umano. Per la sua durata, il gioco richiede, in breve, di impegnarsi nei valori, nelle valutazioni e nelle preferenze di un virus, un parassita o una scimmia.

Di conseguenza, nonostante le prime apparizioni, Plague Inc. non è, a dir poco, Misantropico, almeno come viene tradizionalmente usato il termine. Piuttosto, prevede modalità non antropocentriche di opposizione all’umanità, respingendo la patologizzazione del Misantropo e la normalizzazione dell’essere umano. Intuisce, infatti, che l’identificazione del sé antroponormativo è essa stessa una forma di scontro e di valutazione piuttosto che un’identità di specie necessaria e inevitabile, e ospita la possibilità di una Misantropia senza umanità.

ZOON POLEMIKON

Senza dubbio, la caratteristica teorica più popolare del pensiero hobbesiano è il cosiddetto pessimismo antropologico, spesso frainteso come onnipresente nel suo lavoro. Tale pessimismo è sostanzialmente correlato a una visione della

natura umana descritta in termini di conflitto costitutivo per la coesistenza tra simili. O, più precisamente, dotato di una capacità naturale di far nascere un tale conflitto, una capacità che nei processi del fluire umano necessariamente, verrà combattuto, se nulla viene contenuto; per ogni uomo, così disposto dalla natura, in lotte secondo il particolare interesse immediato.

E nella nuda natura, nulla deve contenere una cosa del genere: beh, al contrario, il naturale è proprio quell'esibizione di passioni umane che genera la contesa. L'accurata rilevazione di questo aspetto originale, di questo potere innato, di questa possibilità di far esplodere il dissidio e la struttura cruda in cui vive, finisce per risultare, per così dire- e per usare un'espressione che Hobbes stesso avrebbe senza dubbio ipotizzato- una sorta di fortuna. Da questo assioma dal quale verranno dedotti, senza andare oltre, teoremi che impongono di cercare la pace "per un mezzo di conservazione degli uomini in moltitudini" (" for a means of the conservation of men in multitudes ".

L'argomento teorico di Hobbes, basato sull'autoconservazione come causa principale naturale delle azioni umane, salva abilmente lo hiato tra la sfera descrittiva e normativa di questi due elementi: la tensione essenziale tra l'inevitabile guerra primaria di tutti contro tutti e una disposizione naturale per preservare la propria vita, allo stesso tempo spiega e giustifica l'innalzamento della persona artificiale (persona immaginaria), lo Stato, che, dotato artificialmente di potere sovrano (superaneus), è in grado di salvaguardare questa pace dalla guerra. Anche la vecchia nozione aristotelica dell'animale politico (zoon politikon) fallisce.

L'idea del bruto (contenuta in due delle frasi più popolari della letteratura hobbesiana: l'uomo è un lupo per un altro uomo (Homo homini lupus), e lo stato della natura come una guerra di ogni uomo contro ogni uomo (bellum omnium contro omnes), che ha già notevolmente alleviato l'apparizione di De

Cive, sostiene gran parte di ciò che viene rivendicato nel Leviatano, in cui è precisamente un grande artefatto (artefatto), lo Stato, nella forma di un dio mortale e creato da mortali, colui che proteggerà gli uomini dagli uomini, rendendoli dei per gli altri uomini – come segnala la sentenza ignorata e ripetuta di quello che accade: l'uomo è un dio per l'uomo (Homo homini deus).

Un altro degli aspetti rivoluzionari del pensiero hobbesiano (a causa della condizione di rottura radicale con un elemento radicale di Legge e politica) è la concezione della legge naturale, apertamente contraria alla legge tradizionale. L'equalizzazione della legge e del potere nell'ambiente naturale comporta, come conseguenza naturale, la legittimità di qualsiasi atto di predazione nelle condizioni della natura. E finirà per defluire (insieme all'intero edificio politico), quasi per necessità logica, quasi come una concezione positivista del Diritto la cui forza e influenza continuano ad operare ancora oggi. Quindi, e in questo stesso quadro, che il Diritto rimane come ius, se si vuole, anche se non in così tanti accomodamenti (o in comune: non finché ci si rimane accanto) rispetto ai canoni predatori trascendenti (teologici o metafisici), ma, data l'origine naturale limitata come solo dal potere animale, e dopo il corrispondente (perché da quell'origine solo un tale diritto può rimanere) salto umano, civile, politico (con l'accordo come chiave e la figura del sovrano come esecutore), il Diritto rimarrà come adattamento alle volontà convergente degli uomini, un desiderio dopo una deliberazione che è volontariamente concordata.

Questo nuovo adeguamento, questa fissazione del diritto politico consisterà nel determinare il complesso trasferimento, da parte degli accordatori, da parte del diritto naturale originale: un incarico che dipenderà, alla radice, dalla volontà di quegli accordatori, e che dipenderà, a sua volta, dai desideri consigliati dalla ragione, che, legata al desiderio e al servitore di questo (mai sovrano,

perché la ragione non governa, non decide l'azione, consiglia solo, che non è poco) progetterà quella volontà.

Questa legge del desiderio effettivo consigliato dalla ragione, la legge della volontà che governerà gli accordi che sanzionano una legge così speciale, una legge molto indipendente (dal momento che non vi è domino trascendente, che precede chi la detta), una legge dipendente (perché ha confini chiaramente delimitati, gli stessi di quelli della libertà umana già civilizzata: il potere naturale e l'accordo convergente che lo vincolerà) è la fonte del diritto civile, che scaturisce da quella peculiare fonte di diritto naturale descritta da Hobbes. Dove non esiste un canone trascendente, rimarrà solo l'immanente, volontà che fluisce dallo stesso mondo in cui è posto. Hobbes aggiunge al complesso una transizione molto abile tra la fase descrittiva e la fase normativa, che cattura l'essenza di entrambe: ciò che è e ciò che dovrebbe essere, a seconda di questo (una volontà inquadrata nei bisogni corrispondenti che, attraverso l'accordo-promessa , determina cosa dovrebbe essere). In realtà, assumerà in De corpore, l'intera causa dei fenomeni come equivalente al pieno potere, che li differenzia, solo, nell'occhio umano che guarda al passato o al futuro.

Per quanto riguarda le leggi della natura (laws of nature) la rivoluzione non è da meno: si potrebbe dire che per Hobbes le leggi della natura sono poco più (o niente di più) che dei consigli per la sopravvivenza del – questo sì – migliore dei consiglieri nella migliore disposizione retorica: la ragione, e sotto forma di conclusioni o teoremi. Un consiglio appreso, veritiero, molto accurato e molto efficace, se si segue l'idea di Hobbes: ma senza alcun mandato di qualità, senza agenti legittimati dalla volontà comune che agisce di conseguenza, in caso che tali leggi non siano rispettate. Queste leggi non possono essere interpretate, nella loro dottrina, come precetti assolutamente imposti, come di solito accadeva e continua ad accadere in larga misura. Cioè, non sono

fissazioni di matrice aliene alle condizioni precedenti, assolutamente emancipate in virtù della loro assoluta pre-incorporazione, indipendenti da condizionali o coniugate, liberate dall'estremità molto concreta e banale che le rende ragionevoli: sono più teoremi che assiomi, per tradurlo in termini logici-matematici, come afferma Hobbes, a differenza della tradizione: sono dedotti. Che la pace debba essere cercata come un bene autonomo non è scritto da nessuna parte: ne consegue che, dato il desiderio di autoconservazione che determina la condizione umana, il modo migliore per viverla, è perseguire la pace. Lo status di consigli di lega (ob-lega, se preferiamo) a questi teoremi è l'elemento chiave: il condizionale, quello per il quale dipenderà, in buona logica (la ragione giusta (ragione hobbesiana [right reason]), e solo nella validità. Nel caso in esame, tale condizione di base è la conservazione.

La natura controversa di questo punto, per quanto riguarda ciò che stiamo cercando di dire ora, è arginata. L'assioma può fallire, se si vuole, ma ciò non influisce sulla struttura dell'argomento, l'idea che difendiamo: la condizione dei teoremi, quindi dipendente dai loro assiomi corrispondenti, dalle leggi della natura. La condizione, in breve, di consigli ad hoc per fare la nostra volontà terrena. Il legame, perfettamente de-teologizzato e costitutivamente insostituibile, con l'ultima volontà (last will): ecco perché sarà inalienabile (inarrestabile) diritto della natura, anche già nella sfera civile: la conservazione, che è la propria, vita non trasferibile di ciascuno.

Non vi è alcun diritto perché la legge è caduta – la libertà del soggetto è quella che viene data nonostante gli ordini sovrani e non in loro assenza – ma questo perché la legge non può fermare o arrestare il movimento dell'impulso vitale e, tanto meno, i modi vitali che sono in essi-correlazione. Come mostra il dettaglio dell'illustrazione di copertina che accompagna notoriamente il Leviatano: si celebra una battaglia

mentre tutto sembra ancora dinnanzi all'imponente immagine del dio mortale. Hobbes sembra voler ricordarci che quando tutto sembra immobile, le cose si muovono ancora.

In breve, la svolta hobbesiana non consiste solo o esattamente nel fornire visioni radicalmente diverse (con una radicalità che non ha eguali nella storia del pensiero, ci sembra) ai problemi classici (e, da ciò che si vede, eterno: tocca l'osso, diremmo), anche se: possiamo trovare ovvi antecedenti nella tradizione materialista-atomista-epicureo in particolare, in Ockam, Marsilio, Bodin e Machiavelli. Il grande contributo di Hobbes, quindi, consiste piuttosto nell'acuta motivazione che dà di ciò, piuttosto che nella dipartita, come avveniva una volta, è la conclusione, nel più puro stile geometrico; e, soprattutto, come, da banali fissi assiomatici, sviluppa e conclude posture radicali. Nel caso di Menchaca questo sembra particolarmente valido: diritto e potere naturale, partenza, equivalente, e Hobbes, seguiranno questa linea intrapresa. Fondazione e conclusione, radicalmente diverse: Menchaca fonda in Dio; Hobbes, in questo mondo, fuori dal quale non c'è nulla.

Per gli spagnoli, la Legge, è sanzionata e ordinata da Dio; secondo l'inglese, la Legge, è nient'altro che una cosa di uomini, dove non entra più Dio (per così dire) nelle leggi della natura (in senso fisico) e nelle condizioni dell'uomo desiderante, che recita la sua volontà solo vincolata da quelle leggi e da quelle che egli costruirà da lì in poi. La natura costruttiva di queste ultime, tuttavia, sarà molto diversa da quelle di quegli: poiché non è perduta, come Skinner (2008) sembra assumere, la libertà naturale: piuttosto è condizionatamente data, il che è una cosa molto diversa, perché può essere recuperata quando si vuole (uccidere è facile, come disobbedire, infrangere, cospirare …), anche (aumenteranno la volontà e il potere, e con loro il problema politico) indipendentemente dal fatto che la condizione sia soddisfatta o meno. La natura civile di quella costrizione,

per scopi perfettamente pertinenti, non ha nulla a che fare con il carattere naturale di quella: che usare la legge in modo intercambiabile per entrambi i fenomeni può essere fonte di confusione (in effetti lo è); che non rileviamo quella chiave confusa, pertinente, a questo livello, fatale.

ANONIMATO (GUIDA)

Ricevo e pubblico: Interessante guida sulla sicurezza elettronica, che alla fine, è un "mezzo per raggiungere un fine" (il Nostro naturalmente):

guida2

guida3

guida4

Con MEGA

Guida2

https://mega.nz/#!7jJzQIpQ!2slIbOP3e78k6Y_kiWGDP6NvW4jZHFDIs6AHrdZjPrM

Guida3

https://mega.nz/#!P7JFnAgI!cD9R2dlSa7sclbBI2gZON-x8wZHe1mJ-5fjiZwM7Ryw

Guida4

https://mega.nz/#!KuA1jSrQ!hAx_R12FOGRZAvBAWG8Y30xIkSVIKR2pfqSdgTOef34

CRITTOGRAFIA AUTO-PRODOTTA INACCESSIBILE DI PENNA E CARTA

Ricevo e pubblico dagli affini di "Terrorismo Egoarca", questo nuovo lavoro editoriale, e di propaganda illegalista/estremista-"Tutto è Permesso":

http://terrorismoegoarca.torpress2sarn7xw.onion/2019/08/08/crittografia-auto-prodotta-inaccessibile-di-penna-e-carta/

https://upload.disroot.org/r/JiJyXg4y#xsJdrv9BxhaeqbGa14VEYTo4bltn0wgYIodeRKi81lE=

Oggi siamo circondati da un'enorme potenza computazionale e da vasti sistemi di comunicazione. Quando visiti il sito della tua banca, non pensi alla transazione di chiavi crittografiche e alla verifica delle firme digitali. Quando parli al cellulare, non devi preoccuparti del COMSEC (presumibilmente).

Non molto tempo fa, tuttavia, un "computer" era una giovane donna alla scrivania e i collegamenti crittografici erano brevi messaggi. In questo articolo, ti mostrerò uno schema di crittografia comprovato e inaccessibile. che può essere fatto con carta e penna. Se correttamente implementato, la crittografia "taccuino monouso" può essere utilizzata praticamente su qualsiasi supporto ed è ancora utilizzata dalle "black helicopter organizations" per condurre missioni all'estero.

Storia

Quella che ora chiamiamo crittografia “taccuino monouso”(OTP, in inglese) è stata brevettata da Gilbert Vernam presso l’AT&T nel 1919 e migliorata dal Capitano Joseph Mauborgne del Signal Corps dell’esercito. La prima applicazione militare fu riportata dalla rivista tedesca Kurzwellenpanorama nella prima guerra mondiale. Successivamente fu impiegata dalla BBC per inviare messaggi in codice agli agenti delle operazioni speciali all’estero.

La più estesa applicazione OTP è stata quella sulle stazioni numeriche; queste stazioni radio a onde corte senza licenza e misteriose iniziarono a trasmettere durante la Guerra Fredda e sono funzionanti ancora oggi. Con un hardware comune ed economico, un agente in qualsiasi parte del mondo può usare una trasmissione dalla propria organizzazione in modo non rintracciabile e inaccessibile. Queste postazioni riproducono spesso introduzioni musicali seguite da un codice Morse o registrazioni vocali che leggono un codice alfanumerico. Il progetto Conet ha svolto un lavoro straordinario mettendo insieme 30 anni di registrazioni di queste postazioni e un opuscolo informativo per il download gratuito. Se ti piacciono i giochi di spionaggio, assicurati di provarlo.

Esempio

Userò l’esempio di una spia Sovietica. A Mosca, ti viene rilasciato un piccolo libretto di sequenze di numeri casuali etichettati; questo quaderno crittografico è identico a quello che hanno gli operatori delle postazioni numeriche. Lo cuci nel tuo abito e lo introduci di nascosto nella Germania occidentale. Mentre sei lì, acquisti una radio ad onde corte e, nella riservatezza del tuo appartamento, ascolti il tempo e la frequenza predeterminati. Dopo una serie di segnali acustici, senti il tintinnio della musica che verifica che stai ascoltando la stazione corretta.

Si sente una voce Russa e ti dà otto numeri (mostrati nella tabella qui sotto). Usando i primi due per identificare quale

codice utilizzare, unisci il tuo messaggio crittografato con la tua chiave per decodificare il nome del tuo contatto, "Egorov". Strappi la pagina dell'opuscolo chiave e la butti nel camino.

Ecco l'esempio dall'alto in forma matematica. Il testo crittografato è ciò che è arriva alla radio, la chiave è ciò che era nel tuo libro.

Prendi il tuo testo crittografato (01-03-09-07-24-11) e aggiungi la chiave dal tuo libro (04-04-06-11-17-11). Nota che la posizione cinque è il testo cifrato e la somma della chiave su 17, non 41. Poiché ci sono solo 26 lettere, "ruota" attorno per farlo diventare 15 (24 + 17 = 41. 41-26 = 17). Il processo di crittografia presso la posizione numerica ha semplicemente preso il messaggio (EGOROV) e sottratto la chiave casuale da esso, usando lo stesso metodo di rotazione per i numeri negativi.

Se la chiave è scientificamente casuale, in teoria, il codice è impossibile da decifrare. Questo perché non esiste alcuna correlazione tra il modo in cui la prima E è crittografata e la quinta, e un codice di tre lettere potrebbe essere altrettanto facilmente "CAT" o "DOG". Una chiave OTP viene utilizzata una sola volta e ha una chiave lunga quanto il messaggio; se una chiave viene riutilizzata, è possibile usare un attacco computazionale e decifrarlo. Eseguito correttamente, nessun messaggio antecedente viene compromesso se una singola chiave viene rotta (diversamente da AES o PGP). Inoltre, mantenendo l'intero processo su carta, si riduce al minimo il numero di meccanismi che devono essere protetti e quindi si riducono i vettori di attacco. Con cinque minuti di applicazione, si può adottare lo stesso sistema alle conversazioni di messaggistica istantanea, e-mail, radio a onde corte stazioni o SMS. Infine, gli umani comprendono intuitivamente se e come nascondere e proteggere le cose, ma

dall’altra comprendono solo concettualmente i firewall e SSL.

Una limitazione di OTP, significa che esiste un numero finito di messaggi che possono essere inviati prima che sia necessario scambiare una nuova serie di chiavi. Inoltre, lo scambio di chiavi deve avvenire fuori banda e in genere di persona; questo rende il sistema più scomodo rispetto a PGP o AES per le comunicazioni di rete del computer. Comprendendo questi limiti e vantaggi, è possibile creare facilmente la propria implementazione crittografica.

Costruisci il tuo sistema

Passo 1 – Decidi un Alfabeto

Innanzitutto dobbiamo capire come interpretare i messaggi decrittati come inglese. Spesso i messaggi vengono convertiti in numeri usando per facilità di calcolo l’OTP. I numeri non devono rappresentare solo lettere, come nell’esempio precedente, ma anche numeri, simboli, parole e sintassi. Sebbene questo alfabeto non sia sensibile, di per sé, di solito è preservato con le tue chiavi. Ecco un esempio di alfabeto che ho creato per i messaggi di testo.

Passo 2 – Genera il tuo Libro Chiave

Ora dobbiamo generare il libro chiave per entrare clandestinamente nella Germania occidentale. A differenza della CIA di Hoover, generare 10.000 nuovi numeri scientificamente casuali non richiede una stanza piena di agenti che lanciano dadi per una settimana. RANDOM.org è un servizio gratuito gestito dal dipartimento di informatica del Trinity College di Dublino, in Irlanda; i loro numeri casuali sono generati dal rumore atmosferico ed è un’approssimazione più vicina ai numeri casuali che puoi ottenere senza un pezzo di uranio e un contatore Geiger.

Usa il loro generatore di numeri interi con crittografia SSL per raccogliere le proprie chiavi di crittografia. I modi più sicuri per raccoglierli sono utilizzare la modalità di navigazione privata di Firefox, la finestra di Google Incognito o crittografare il disco rigido. Se usi software per fogli di calcolo come Excel, assicurati di disabilitare il salvataggio automatico se il tuo disco rigido non è crittografato. Stampa questo e consegnalo al tuo compagno, preferibilmente su una stampante senza punti segreti del numero seriale. Al termine, il tuo libro chiave avrà pagine con numeri a due cifre etichettati

Passo 3 – Trasmettere

Quando trasmetti, hai molte opzioni a tua disposizione oggi. La tua radio tascabile crittografata (cellulare) e SMS connessa a livello globale sono fantastici sistemi, anche se esponi la tua posizione geografica al fornitore di servizi. Se desideri trasmettere un messaggio a molte persone / agenti, un account Twitter o Blogger inviato attraverso Tor o un cellulare prepagato crea l'equivalente moderno di una posizione numerica. In effetti, esiste almeno una rete bot nota coordinata tramite un account Twitter anonimo (non crittografato, tuttavia).

Questo è tutto, non sono necessari altri strumenti o formazione. Sebbene OTP abbia certamente i suoi limiti, nelle giuste circostanze può superare i sistemi crittografici più sofisticati (e più difficili). Chiunque abbia cinque minuti di formazione, un pezzo di carta può usare gli stessi strumenti che la CIA, il KGB e il Mossad usano per condurre operazioni all'estero. Sta a te capire come applicarli nella propria condizione, ma ricorda che molte volte, lo strumento più semplice nel tuo arsenale è il più potente.

Semplice crittografia dei file utilizzando "taccuino monouso"

e OR esclusivo

“Come ho imparato ad amare le operazioni logiche bit a bit in C.”

di
Aegis (Glen E. Gardner, Jr.)
Aegis@www.night-flyer.com
ggardner@ace.cs.ohiou.edu
per
C-scene Magazine

Iniziamo

L’arte nera della crittografia mi ha sempre esterrefatto. Si tratta di occultamento e inganno. Nascondere le informazioni in bella vista rendendole un lavoro troppo confuso, troppo complicato o troppo lento perché gli stronzi possano decifrarlo.

Esistono numerosi schemi di crittografia resistenti al mondo che funzionano bene. Negli ultimi anni, sempre più di questi hanno fallito, perché attaccati da programmatori persistenti armati di combinazioni sempre più sofisticate e potenti di hardware e software.

Con la crescita quasi esponenziale della velocità e della potenza del software e dell’hardware di oggi, si ha comprensibilmente l’impressione che nessun sistema sia sicuro e che quasi nessuno schema di crittografia sia impenetrabile.

Quasi inaspettatamente, ci sono alcuni metodi di crittografia sorprendentemente semplici che sono davvero validi. In effetti, se usati con attenzione, sono “sicuri” come qualsiasi altra cosa. Uno di questi schemi (quello che tratterò qui) prevede logicamente ORing dei byte in un file di destinazione con numeri generati casualmente, risultando in un file crittografato. Questo schema viene spesso chiamato “OTP”, o “taccuino mono-uso”, perché genera una chiave una sola volta.

Ecco come funziona

Useremo un bit a bit EXCLUSIVE OR, XOR per eseguire la crittografia. XOR imposta il risultato su 1 solo se uno dei bit è 1, ma non se entrambi sono 1

Ecco un estratto da "ANSI C PROGRAMMING" di Steven C. Lawlor, West Publishing, ISBN 0-314-02839-7 dalle pagine 316.317

BIT A BIT EXCLUSIVE OR

Utilizzando l'OR esclusivo bit a bit o XOR bit a bit (^), il bit risultante è 1 se uno dei bit esaminati, ma non entrambi, sono 1. In altre parole, se i bit sono diversi, i risultati saranno 1. Risultati del campione da valore1 ^ valore2 sono:

```
valore1 00110100 10111000 11000010
^ valore2 01000110 00001100 10001100
= risultato 01110010 10110100 01001110
```

XOR ha tre proprietà interessanti. Innanzitutto, qualsiasi valore XORed con se stesso (valore ^ valore) si tradurrà in zero.

```
valore 00110100 10111000 11000010
^ valore 00110100 10111000 11000010
= risultato 00000000 00000000 00000000
```

Questo schema può essere usato come test per la corrispondenza; valore1 ^ valore2 è zero se i valori sono uguali. I programmatori di linguaggio assemblati talvolta usano questo come metodo per impostare un valore su zero, poiché è leggermente più efficiente di un compito diretto. Poiché la chiarezza del programma è, nella maggior parte dei casi, più importante dei piccoli aumenti di efficienza, probabilmente dovremmo usare valore = 0 anziché valore ^ = valore.

Una seconda proprietà è che un valore XORed due volte con un valore specifico ritorna al valore originale. L'espressione

valore1 ^ valore2 ^ valore2 è sempre uguale a valore1.

valore1 00110100 10111000 11000010
^ valore2 01000110 00001100 10001100
= 01110010 10110100 01001110
^ valore2 01000110 00001100 10001100
= risultato 00110100 10111000 11000010

Questo viene talvolta utilizzato come parte di una semplice routine di crittografia. Per crittografare i dati ogni byte è XORed con un byte di crittografia specifico. Per decrittografarlo, i dati vengono sottoposti allo stesso processo

Trasportando questo un ulteriore passo, si può usare quanto segue per scambiare due valori senza la necessità di una variabile temporanea.

```
valore1 ^= valore2;
valore2 ^= valore1;
valore1 ^= valore2;
```

Una terza proprietà è che qualsiasi bit XORed con 1 bit verrà invertito. Questo
viene utilizzato per attivare / disattivare i bit: impostarli su 0 se fossero 1 o 1 se fossero 0. Gli esempi seguenti attivano i bit due e sei …

valore 10010100 00111011 11001010
^ azione 01000100 01000100 01000100
= risultato 01010000 01111111 10001110

E questo è tutto ciò che prenderemo in prestito dal signor Lawlor oggi …

Su questo programma

Il programma apre la chiave e i file sorgente, legge un byte da entrambi, XOR è i due numeri insieme, quindi salva il risultato nel file di destinazione. Il processo viene ripetuto

fino al raggiungimento della fine del file di origine. Se la chiave predefinita è stata trovata in fase di esecuzione, non viene creata una nuova chiave e il programma utilizza la chiave predefinita esistente. Al termine, la chiave predefinita viene eliminata. Se non viene trovata alcuna chiave predefinita e non è stato fornito alcun nome chiave sulla riga di comando, prima della crittografia verrà creata una chiave predefinita e non verrà eliminata. Allo stesso modo, se nella riga di comando è stata fornita un nome chiave, la chiave non verrà eliminata al completamento del programma.

Il programma richiede una chiave della stessa lunghezza del file di origine. Se non viene trovato un file, viene generata una chiave adatta. Ogni byte della sorgente è XORed con un byte dalla chiave e salvato nel file di destinazione. Nel caso della chiave generata dal programma, i numeri pseudocasuali vanno da 0 a 255d. Puoi usare qualsiasi file come chiave, ma devi prestare attenzione. I byte del file chiave con il valore decimale 0 non crittograferanno l'origine. Potrebbe essere meglio usare un capitolo della Sacra Bibbia, o Principia Discordia come chiave, piuttosto che usare un binario. In caso di dubbio, utilizzare il programma per generare una chiave pseudo-casuale.

Usando il programma

L'utente immette il nome del file di origine, il nome del file di destinazione e il nome della chiave da utilizzare. Il programma utilizza la chiave per crittografare il file di origine e, se non viene fornito alcun nome chiave, genera una nuova chiave utilizzando un generatore di numeri psuedo-casuali, che è stato inserito dall'orologio in tempo reale. I dati crittografati vengono quindi salvati nel file di destinazione..

Per decrittografare un file, è necessario disporre del file crittografato e della stessa chiave con cui è stato crittografato. Eseguire il programma, fornendo il nome del

file crittografato, seguito dal nome del file di destinazione desiderato e dal nome del file chiave. Il file non crittografato verrà quindi salvato come file di destinazione. Se non è stato fornito alcun nome chiave al programma, esso cercherà una chiave chiamata "nuova chiave" e la utilizzerà. Se "nuova chiave" esiste (è necessario se si utilizza l'impostazione predefinita e si desidera decrittografare), verrà utilizzato e quindi eliminato.

Probabilmente dovrai conoscere il nome del file originale e l'estensione del file, poiché il programma di crittografia non ne tiene traccia.

Se non viene specificato alcun nome per la chiave o il file non viene trovato, il programma genererà una chiave propria, usando numeri pseudocasuali. Se il programma trova una chiave con lo stesso nome del nome predefinito (nuova chiave), utilizza il file esistente, quindi lo elimina per impedire il riutilizzo della chiave.

Errori e Particolarità

ll programma ti consentirà di utilizzare una chiave più corta della sorgente. Ciò significa che, una volta raggiunta la fine del file chiave, tutti i byte di origine rimanenti verranno crittografati con lo stesso valore chiave (FFh), rendendo probabilmente una parte del file facile da decifrare. ASSICURARSI CHE LA CHIAVE SIA GRANDE COME LA SORGENTE O PIÙ GRANDE.

L'uso delle chiavi è una cosa negativa. Poiché il computer non è in grado di generare numeri casuali "veri", esiste un modello per i numeri pseudocasuali che genera. L'uso ripetuto di una chiave offre ai cracker la possibilità di scoprire la chiave facendo alcune ipotesi sul contenuto di un file. Se ottengono abbastanza file che usano la stessa chiave, quasi sicuramente finirai per essere decifrato. NON RIUTILIZZARE LE CHIAVI!

C’è il pericolo che la crittografia di file molto lunghi possa renderli più facili da decifrare a causa della leggera tendenza di alcuni generatori di numeri casuali a ripetere eventualmente una sequenza di numeri “casuali”. Quindi, fai attenzione a crittografare file molto grandi a meno che tu non sappia che la tua chiave è veramente “casuale”.

Questo programma è stato compilato su FreeBSD usando GCC e Windows NT 4.0, usando BC5.01. Gli utenti Linux o OS / 2 non dovrebbero avere problemi a compilare la sorgente. Gli utenti DOS saranno probabilmente in grado di farlo funzionare con un minimo di problemi, ma consiglio vivamente che quegli utenti passino a un sistema operativo a 32 bit.

```
*/
/* CRYPTIC.C V 1.0 Copyright 1998 by Glen E. Gardner, Jr. */
/* Crittografa un file usando una chiave casuale e salva la chiave. */
/* Genera automaticamente una nuova chiave quando necessario. La nuova */
/* la chiave viene eliminata al secondo utilizzo (decrittograficata) per impedire */
/* riutilizzo accidentale della stessa chiave per la crittografia.*/
/* Questo programma è freeware, usalo liberamente e godine! */

/* Assicurati di citare l’autore e includere l’originale */
/*fonte in tutte le distribuzioni. */
/* Scritto e compilato in ANSI C usando Borland C++ V 5.02 */
/* Testato su Windows NT 4.0 e FreeBSD 2.2.5 (usando gcc). */
/* Esegui questo programma una volta per crittografare e di nuovo, usando il*/
/* stessa chiave, da decriptare. */
/* Qualsiasi file può essere utilizzato come chiave purché sia il file */
/* stessa dimensione (o più grande) del file crittografato. */
/* (le chiavi piccole e ripetute sono per i WIMP) */
/* Devi stare attento a ciò che usi come chiave. Sei tu */
```

```
/*se non ci credi, prova a crittografare un file usando
Windows */
/* file dll come chiave e guardando l'output con un testo*/
/* editor. */
/*L'output crittografato è binario. Puoi usarlo come
criptato*/
/* cripta ogni file. */

#include<stdio.h>
#include<stdlib.h>
#include<time.h>

/* Use questo include con GCC sulla macchina FreeBSD machines.
*/
/* #include</usr/include/sys/stat.h> */

/* Utilizzare questo include invece di quello sopra per
Windows NT. */
#include<sys\stat.h>

void makekey(long int,char *);

int main(int argc,char **argv)
{

struct stat statbuf;

time_t t;
int key;
int data;
int output;
int count=0;
int FLAG=0;
FILE * mykeyfile;
FILE * sourcefile;
FILE * destfile;

if(argc<3)
{
```

```
printf("CRYPTIC Coyright 1998 by Glen E. Gardner, Jr.\n");
printf("USE: CRYPTIC
<DESTINATION> <KEY>\n");
return(0);

}

/* Da notare che se non viene fornito alcun nome chiave, il
programma genera e utilizza una nuova chiave */
/*Assicurarsi che sia presente la chiave esatta durante la
decodifica (duh). Non il programma*/
/*Si deve sapere se si sta crittografando o decrittografando.
Rosicchia semplicemente il file sorgente con */
/*qualunque chiave abbia sputa il risultato. */

/*Esegui il salvataggio se viene utilizzato il numero errato
di argomenti. */

if(argc>4){printf("Too many arguments.");return(1);}

/*Semina il generatore di numeri casuali per un uso
successivo. */
srand((unsigned) time(&t));

/* ottieni la dimensione del file di origine */
if ((sourcefile = fopen(argv[1], "rb"))== NULL)

{

printf("Can't open source file.\n");

return(4);
}

fflush(sourcefile);

fstat(fileno(sourcefile), &statbuf);

fclose(sourcefile);

/* Cerca il file chiave predefinito se non ne viene fornito
```

```
nessuno */
if(argv[3]==NULL){argv[3]=”newkey”;}

/* Se la chiave non viene trovata, crearne una nuova. */
if ((mykeyfile = fopen(argv[3], “r”))== NULL)

{

FLAG=1;
printf(“Can’t open key file.\n”);
printf(“Making a new key…\n”);
makekey(statbuf.st_size,”newkey”);
}else{fclose(mykeyfile);}

/* open all the necessary files. */
mykeyfile=fopen(argv[3],”rb”);
sourcefile=fopen(argv[1],”rb”);
destfile=fopen(argv[2],”wb”);

/* Utilizzare la chiave per crittografare / decrittografare il
file di origine. */
while (count < (statbuf.st_size))

{
key=fgetc(mykeyfile);
data=fgetc(sourcefile);
/* Questo è tutto ciò che c’è da fare. */
output=(key^data);
/*XOR il byte di dati una volta con un byte da una chiave e
crittografa . */
/*XOR di nuovo il byte risultante con lo stesso byte della
stessa chiave e decodifica. */
/* scrivere il risultato nel file di output. */
fputc(output,destfile);
count++;
}
/* chiudi il files. */
fclose(mykeyfile);
fclose(sourcefile);
```

```
fclose(destfile);
/* Elimina la chiave predefinita la seconda volta per impedirne il riutilizzo. */
/* La chiave viene eliminata solo se non è stata specificata una chiave e se l'impostazione è predefinita*/
/*la chiave non è nuova. */

if(FLAG==0)

{

/* usa questo con Windows NT */
system("erase newkey");

/* use questo con FreeBSD */
/* system("rm newkey"); */

}

return(0);

}

/* MAKEKEY() crea una chiave usando numeri casuali. */
/* Il generatore di numeri casuali viene trasmesso dall'orologio in tempo reale. */
/*È abbastanza casuale, ma la natura del generatore pseudocasuale non lo è*/
/* completamente casuale. Ciò significa che sarà un programmatore intelligente*/
/* alla fine rompi la chiave. */
/* Non riutilizzare le chiavi e considerare di investire tempo in un modo migliore di generare */
/*stringhe di numeri casuali da utilizzare come chiave. */
void makekey(long int size,char *name)

{

int byte;
int count=0;
```

```
FILE * filein;

filein=fopen(name,”wb”);

while(count&lt;size)
{
byte=rand() % 256;
fprintf(filein,”%c”,byte);
count++;
}
fclose(filein);
}
```

Le leggi della crittografia:

Crittografia perfetta: Il “taccuino monouso”

Il Cifrario di Cesare.

Le persone hanno usato la crittografia per migliaia di anni. Ad esempio, il Cifrario di Cesare, che fu usato durante il periodo di Giulio Cesare, avvolge l’alfabeto dalla A alla Z in un cerchio. Il metodo impiega uno spostamento fisso, diciamo di 3, per trasformare A in D, B in E, e così via fino a quando da W a Z, da X a A, da Y a B e da Z a C. Pertanto, un messaggio ATTACK diventa DWWDFN e appare incomprensibile per qualcuno che intercetta il messaggio. All’altro capo, si può invertire la trasformazione facendo 3 lettere nella direzione opposta per riportare DWWDFN in ATTACK.

Questo esempio illustra molti concetti e terminologie della crittografia. Il messaggio originale è anche chiamato testo in chiaro. Il messaggio trasformato è anche chiamato testo cifrato o messaggio crittografato e il processo di creazione del testo cifrato è crittografia. Il processo di recupero del messaggio originale viene chiamato decrittografia, utilizzando un algoritmo di decrittografia. Quindi si decodifica il testo cifrato.

Il metodo di base utilizzato, spostando una distanza fissa attorno al cerchio di lettere, è l'algoritmo della crittografia. In questo caso l'algoritmo di decodifica è essenzialmente lo stesso. La distanza specifica spostata, 3 in questo caso, è la chiave per questo algoritmo e in questo tipo di sistema di chiavi simmetriche, la chiave è la stessa sia per la crittografia che per la decrittografia. Di solito l'algoritmo di base non è tenuto segreto, ma solo la chiave specifica. L'idea è di ridurre il problema di mantenere un intero messaggio sicuro al problema di proteggere un singolo tasto di scelta rapida, seguendo la Legge C1 dell'Introduzione alla crittografia.

Per questo semplice algoritmo ci sono solo 26 chiavi possibili: le distanze di spostamento di 0, 1, 2, ecc. Fino a 25, anche se 0 lascia invariato il messaggio, quindi un tasto uguale a 0 non manterrà molti segreti. Se la chiave è maggiore di 25, basta dividere per 26 e prendere il resto. (Quindi le chiavi formano solo l'intero modulo 26, il gruppo Z26 descritto nella sezione preferiti dei Crittografici)

Se un intercettore di questo messaggio sospetta la natura dell'algoritmo utilizzato, è facile provare ciascuno delle 25 chiavi (tralasciando 0) per vedere se risulta un messaggio significativo – un metodo per infrangere un codice noto come ricerca esaustiva. In questo caso la ricerca è breve, anche se potrebbe ancora creare problemi se le lettere nel testo cifrato vengono eseguite insieme senza spazi vuoti tra le parole.

Il Cifrario di Cesare è solo una combinazione speciale dei crittogrammi del capitolo precedente, poiché con uno spostamento di 3, ad esempio, la chiave del crittogramma è:

Alfabeto: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Decifrato come: DEFGHIJKLMNOPQRSTUVWXYZABC

Ecco un'implementazione al computer del Cifrario di Cesare:

sorgente Java.

Il Cifrario di Beale.

Il Cifrario di Beale è solo una semplice estensione del Cifrario di Cesare, ma è facile da usare e offre un'eccellente sicurezza.

Considera il Cifrario di Cesare: della sezione precedente e associa le lettere da A a Z con i numeri da 0 a 25, ovvero A è associato a 0, B con 1, C con 2 e così via fino a Z con 25. Si può rappresentare il precedente spostamento di 3 nell'esempio con la lettera D, in modo che ogni lettera specifichi uno spostamento. Uno speciale metodo di crittografia chiamato codice Beale inizia con un testo canone (la chiave in questo caso) come la Costituzione degli Stati Uniti (WE THE PEOPLE…) E con il messaggio da crittografare, ad esempio ATTACK. Annota le lettere del testo comune su una riga, seguite dalle lettere del messaggio sulla riga successiva. In ogni colonna, la lettera superiore viene interpretata come uno spostamento da utilizzare in un Cifrario di Cesare, sulla lettera nella seconda riga. Quindi sotto nella seconda colonna, la E nella prima riga significa che uno spostamento di 4 viene applicato alla lettera T nella seconda riga, per ottenere la lettera X.

Testo comune (chiave): WETHEP
Messaggio: ATTACK
Messaggio criptato: WXMHGZ

La persona che riceve il messaggio crittografato deve sapere qual è il testo canone. Quindi questo ricevitore può invertire la suddetta crittografia applicando lo spostamento nella direzione opposta per recuperare il messaggio originale. Questo metodo gestirà un messaggio di qualsiasi lunghezza semplicemente usando più del testo comune. Si noti che in questo esempio i due Ts sono usciti come lettere diverse nel messaggio crittografato. Per maggiore sicurezza, non si dovrebbe usare un testo canone noto come quello in questo

esempio. Invece il mittente e il destinatario potrebbero concordare su una pagina di un libro che entrambi hanno con loro come inizio del loro testo canone.

In effetti, l'origine storica del cifrario di Beale consisteva in tre messaggi: uno in chiaro e gli altri due criptati. Il primo messaggio crittografato utilizzava l'inizio della Costituzione degli Stati Uniti proprio come sopra, e raccontava di un tesoro sepolto. Il terzo messaggio era quello di dire dove trovare il tesoro, ma non è mai stato decifrato. In effetti, se il testo comune non è noto, può essere molto difficile crittografare un cifrario di Beale.

Tutta la sicurezza di questo sistema risiede nella segretezza del testo comune. Ci sono una serie di insidie sottili con questo metodo, come con la maggior parte della crittografia. Ad esempio, supponi di fare un viaggio in Kazakhstan , e di voler comunicare in segreto con il tuo amico a casa. Acquistate due copie di un romanzo poliziesco economico e concordate una pagina di questo. La polizia segreta del Kazakhstan potrebbe notare il romanzo che stai trasportando, digitalizzare l'intero libro e provare tutti i possibili punti di partenza nel suo testo, come possibili modi per decrittografare le tue comunicazioni. Se ciò non funzionasse, potrebbero provare a prendere ogni terza lettera da ogni punto di partenza o provare altri schemi più complessi.

Ecco un'implementazione al computer del cifrario di Beale: sorgente Java.

Perfetta Crittografia: il "taccuino monouso"

Può essere sorprendente per il lettore che esistano semplici metodi di crittografia " perfetti ", il che significa che esiste una prova matematica che la crittoanalisi è impossibile da agire. Il termine "perfetto" nella crittografia significa anche che dopo che un avversario ha il testo cifrato non ha molte più informazioni rispetto a prima.

Il più semplice di questi metodi perfetti è chiamato il "taccuino monouso". La disamina successiva spiega perché questi metodi perfetti non sono pratici da usare nelle comunicazioni moderne. Tuttavia, per i metodi pratici esiste sempre la possibilità che un ricercatore intelligente o persino un hacker intelligente possano infrangerne il metodo. Anche i crittoanalisti possono rompere questi altri metodi usando ricerche esaustive come quella sulla "forza bruta".

L'unico problema è il tempo necessario per romperli. Con gli attuali potenti algoritmi crittografici, è probabile che non ci siano modi abbreviati per rompere i sistemi e l'attuale crittoanalisi richiede decenni o millenni o più per interrompere gli algoritmi mediante una ricerca esaustiva. (Il tempo di interruzione dipende da vari fattori, tra cui in particolare la lunghezza della chiave crittografica.) Riassumendo, con i metodi pratici non esiste una garanzia assoluta di sicurezza, ma gli esperti si aspettano che rimangano integri. D'altra parte, il "taccuino monouso" è completamente indistruttibile.

Il "taccuino monouso" è solo una semplice variante del Cifrario di Beale. Inizia con una sequenza casuale di lettere per il testo canone (che è la chiave in questo caso). Supponiamo ad esempio che uno utilizzi RQBOPS come testo comune, supponendo che siano 6 lettere scelte completamente a caso e supponiamo che il messaggio sia lo stesso. Quindi la crittografia utilizza lo stesso metodo utilizzato per il Cifrario di Beale, tranne per il fatto che il testo o la chiave canone non è una citazione dall'inglese, ma è una stringa casuale di lettere.

Testo comune (chiave casuale): RQBOPS
Messaggio: ATTACK
Messaggio criptato: RJUORC

Quindi, ad esempio, la terza colonna usa la lettera B, che rappresenta una rotazione di 1, per trasformare la lettera in

chiaro T nella lettera in testo cifrato U. Il ricevitore deve avere la stessa stringa casuale di lettere intorno per la decrittazione: RQBOPS in questo caso. Come parte importante di questa discussione, voglio dimostrare che questo metodo è perfetto finché le lettere del testo canone, sono casuali e tenute segrete. Supponiamo che il messaggio sia GIVEUP invece di ATTACK. Se si fosse iniziato con lettere casuali LBYKXN come testo canone, anziché con le lettere RQBOPS, la crittografia avrebbe preso la forma: Testo comune (chiave casuale): LBYKXN…

Messaggio: GIVEUP
Messaggio criptato: RJUORC

Il messaggio crittografato (testo cifrato) è lo stesso di prima, anche se il messaggio è completamente diverso. Un avversario che intercetta il messaggio crittografato ma non sa nulla del testo comune casuale non ottiene informazioni sul messaggio originale, sia che si tratti di ATTACCO o GIVEUP o di qualsiasi altro messaggio di sei lettere. Dato qualsiasi messaggio, si potrebbe costruire un testo canone in modo che il messaggio sia crittografato per produrre il testo cifrato RJUORC. Un avversario che intercetta il testo cifrato non ha modo di preferire un messaggio piuttosto che un altro. È in questo senso che il "taccuino mono-uso" è perfetto.

In questo secolo le spie hanno spesso usato il "taccuino monouso". L'unico requisito è il testo (il riquadro) di lettere casuali da utilizzare per la crittografia o la decrittografia. La parte che comunica con la spia deve avere esattamente lo stesso testo di lettere casuali. Questo metodo richiede lo scambio sicuro di caratteri a "taccuino monouso": tanti caratteri quanti nel messaggio originale. In un certo senso esso si comporta come la chiave di crittografia, tranne per il fatto che qui la chiave deve essere lunga quanto il messaggio. Ma una chiave così lunga sconfigge un obiettivo della crittografia: ridurre la segretezza di un lungo messaggio alla segretezza di una chiave breve. Se i costi di

archiviazione e trasmissione continuano a diminuire, il "taccuino monouso" potrebbe di nuovo diventare un'alternativa interessante.

Legge PAD1: Il "taccuino mono-uso" è un metodo di trasmissione di chiavi, non un messaggio trasmissione. [Blakeley]

Durante la seconda guerra mondiale i tedeschi usarono una macchina complessa nota come Enigma per la crittografia e la decrittografia. Come evento decisivo della guerra, l'intelligence britannica, con l'aiuto di Alan Turing, il più grande genio del computer del ventesimo secolo, riuscì a infrangere questo codice. Trovo rassicurante pensare che se i tedeschi non fossero stati così fiduciosi nella sicurezza della loro macchina ma avessero invece usato un "taccuino monouso", avrebbero avuto l'irritazione di lavorare con i caratteri di questo, tenerne traccia e rendere sicuro che ogni nave e sottomarino avesse un deposito sufficiente di questi, ma almeno sarebbero stati in grado di utilizzare un sistema completamente infrangibile. Nessuno sa quale sarebbe stato il risultato se gli alleati non fossero stati in grado di violare questo codice tedesco.

Generazione di caratteri casuali per il "taccuino monouso"

Le sezioni successive si soffermeranno maggiormente sulla generazione di numeri casuali, ma per ora basta notare che il "taccuino monouso" richiede una sequenza di caratteri veramente casuale. Se invece si usasse un generatore di numeri casuali per creare la sequenza di caratteri di questo, tale generatore potrebbe dipendere da una singolo causa prima intero a 32 bit per il suo valore iniziale. Quindi ci sarebbero solo 232 diverse sequenze di questi possibili e un computer potrebbe cercarle rapidamente in tutte. Pertanto, se viene utilizzato un generatore di numeri casuali, deve avere almeno 128 bit di causa prima e questo non deve essere derivato esclusivamente da qualcosa come la data e l'ora correnti. (L'uso dell'ora e della data attuali sarebbe di per

sé grave, consentendo una crittoanalisi immediata.)

IL NEMICO E I SUOI DINTORNI

Ricevo e pubblico:

http://informazioneanarchica.altervista.org/pierleone-porcu-il-nemico-e-i-suoi-dintorni/

Non è compito facile, né è comodo il perseverare, quando tutto implica il sapere con se stessi di dover resistere quotidianamente alle piccole soddisfazioni allettatrici del vivere comodo e spensierato. È difficile lottare con costanza mantenendo intatta e incorrotta la propria volontà di non cedere ai compromessi.
La lotta è aspra, dura, aperta, violenta, procura dolore e indurisce i cuori. Molte volte non vi è nulla di piacevole né di soddisfacente, salvo il sapere con noi stessi, che su questa strada passa la nostra autoliberazione individuale e sociale.
Non dobbiamo mai dimenticare che ogni qualvolta si cerca il compromesso, la mediazione in cambio di un po' di tregua, ci si confonde, ci si accosta al nemico che combattiamo, fino a divenire un suo utile supporto, simili in tutto e per tutto a quelle forze che giornalmente lo sostengono.
Come rivoluzionari anarchici, ad ogni momento sosteniamo che non sappiamo concepire soluzioni della questione sociale che non passino per la strada della diretta e radicale distruzione di tutte le istituzioni presenti, ma al di là dei limiti di vaghe promesse teoriche,sono ben pochi i compagni che vanno a verificarle nell'azione.
Si concorda tutti che non si vive di sole chiacchiere, né di

bonarie e ben predisposte affettività ideologiche che ci fanno sentire "tutti fratelli", ma in concreto quello che si fa è poco o nulla.

E i più mirano ad allontanare da sé i rischi e i pericoli che la lotta sempre comporta quando è tale e non ridotta a spettacoli simbolici recitati in piazza. Esiste, nelle situazioni sociali, una vocazione a collaborare,a partecipare per non sentirsi tagliati fuori, con tutte quelle rappresentanze democratiche che sappiamo benissimo quanto concorrano, con la loro azione cloroformizzante, a disarmare e frenare gli impeti della rivolta, a smorzare ogni bisogno della vendetta, a mantener nell'apatia, nella sonnolenza le masse proletarizzate. Così, più che radicalizzare il conflitto sociale tra padroni e schiavi, finiamo per ritrovarci in quel calderone di forze politiche e democratiche che tendono a sanarlo sul terreno della partecipativa e alienante dimensione della collaborazione di classe. Tutto questo è dannoso e letale alla causa sociale rivoluzionaria, che a ogni pie' sospinto diciamo sostenere.

Quel che muove a sdegno e fa rabbia in questo momento, è che alla trista genìa dei ruffiani e sensali e mercanti della carne proletaria, agli impudichi giullari del potere, ai castratori di ogni tensione rivoluzionaria, ai miopi della questione sociale, ai coccodrilli religiosi o laici della non violenza, non si riesca a dare una chiara e precisa risposta.
Anche perché si continua a vivere di bugiarde promesse fatte a se stessi, rattoppando a destra e a manca le proprie manchevolezze, sfuggendo alle proprie contraddizioni, fino ad aderire ad iniziative che non disturbano l'ordine costituito e la terrificante pace sociale che contribuisce a conservarlo.
Quando ogni cosa che si fa appare un igienico laggio volto a sterilizzare preventivamente ogni germe di rivolta, tutto diventa accettabile,anche la merda. Il tutto in cambio di una meschina e miserabile tranquillità socio-domestica.

In una società dove tutti corrono verso il giustificare le

proprie debolezze,dove a prevalere sono i livellamenti verso il basso, dove a dominare sono la mediocrità e la miseria, le coscienze sono flessibili e plasmabili per ogni esigenza, e tutto ciò è espressione di quanto va producendo il sistema democratico.

Nel nostro movimento, molti di coloro che si dicono anarchici, non sono animati da un bisogno intimo di rivolta, ma di essere costantemente afflitti da un mal celato desiderio di voler emergere e possedere una "attraente immagine" come parvenza alternativa ai modelli dominanti nei circuiti sociali della massamarea dei dormienti che ci circonda.
Costoro deviano sul terreno delle piccole felicità, accettano supinamente tutti i compromessi per salvaguardarsi da ogni rischio di conflitto, portano con sé il suicidio di ogni radicale tensione alla rivolta, indossano una umana "maschera" fatta di ipocrite convenzioni e miserevoli giustificazioni, che cela l'aver fatto propria nella tirannia della debolezza, l'abiezione, inconfessabile persino a se stessi nella loro fragilità.

Afflitti dalla paranoia repressiva, sostengono, dietro un contorto e fumoso giro di parole, la tesi che non si deve far nulla in sostanza, al di fuori di quanto legalmente consentito dal sistema, facendosi così apertamente fautori della pacificazione sociale contro la rivolta.
Ma perché non dicono apertamente che hanno paura della lotta,che non sanno dire di no alle proprie debolezze, che il rischio di volersi liberare da ogni tutela li spaventa. Evidentemente preferiscono vivere come animali addomesticati, piuttosto che giocarsi la vita per conquistarsi la libertà. Certo, io li capirei se dicessero chiaramente di amare la comodità, la via dolce e tappezzata di velluto, di non avere il coraggio di rispondere alle angherie ed ai soprusi cui quotidianamente siamo sottoposti.
Tutto ciò è umano; e sappiamo benissimo che "il coraggio uno non se lo può dare". A che serve nascondersi dietro tanta

ipocrisia?

Molti di costoro vivono aggrappati tenacemente ai tanti piccoli miserabili privilegi dati dalla propria condizione sociale, che li vede svolgere diligentemente ruoli dirigenti sui rispettivi posti di lavoro. E così"giocano"a tacere tutto ciò che rovina l'estetica del loro dorato e ovattato mondo in cui se ne stanno ben rintanati, e danno un'immagine addomesticata della realtà del tutto funzionale agli attuali progetti di dominio del capitale e dello Stato.
Non è un caso, che il contrapporsi con durezza di chi si rivolta contro questo stato di cose, si scontri all'interno del Movimento proprio con costoro, che cercano in tutti i modi di dissuaderlo dall'intraprendere la strada dell'insorgenza, volendolo ricondurre all'adozione dei loro innocui e disarmanti metodi di lotta, come l'uso della piazza a mo' di teatro, dove si rappresentano spettacoli simbolici, utili soltanto a dare di se stessi un'immagine perbenista, gratificante e compatibile con quello che è l'andazzo del più generale spettacolo offerto dai network televisivi.

Per altri versi, c'è chi da tempo immemorabile si è lasciato andare al muoversi come uno zombie per forza d'inerzia dentro il circolo chiuso della "militanza-testimonianza", che,alla stregua di un dopolavoro consiste nell'aprire la sede e star lì in attesa di qualche mitico evento, tipo "il risveglio dell'iniziativa di massa"o, nel migliore dei casi, nel diffondere la stampa nei "centri sociali", nelle case occupate e nelle manifestazioni, per poi finire la giornata al cinema o in qualche locale "alternativo", gestito da ex compagni, reduci del '68 o del '77 e dintorni. È in questo modo che si esaurisce, nell'ambito dell'amministrazione-gestione dell'esistente, la dimensione del loro agire, come vuota ripetizione ritualizzata di ciò che è stato e che in quella veste non tornerà mai più. L'accentuarsi della precarietà sociale, l'aggravarsi generalizzato dello stato di cose esistenti, sempre più invivibile, spinge iniziative di lotta

per la difesa del proprio status quo e relegate nella mera sopravvivenza. Sempre più chiusi in questi luoghi della resistenza e della conservazione della propria misera quotidiana, il luogo fisico, è una dimensione-divisa mentale.
Non si criticano le cose che si fanno a partire dal voler dar corso ad una radicalizzazione dello scontro sociale, dal voler dare una maggiore incisività all'azione rivoluzionaria, ma tutto viene criticato a partire da quei tratti caratteriali espressione delle proprie paure e attaccamento alle proprie inveterate abitudini. Si mira soprattutto a non mettere in discussione l'attuale essenza di iniziative, in quanto il farlo comporta il rischio di perdere il piccolo spazio ritagliatosi all'interno del Movimento.
L'illegalismo o meglio il muoversi fuori dalla legge, viene esorcizzato e represso, prima ancora che dagli organi polizieschi e giuridici dello Stato, dai fantasmi che assediano la mente di certi compagni.

Il destino del progetto insurrezionale anarchico, sembra oggi giocarsi attraverso una compiacente adesione data al succedersi di fatti serviti come spettacolo altamente repressivo del potere, che può in questo contare su quella parte di compagni che vogliono con tutte le loro forze che vengano allontanati da sé simili e così pericolosi fantasmi inerenti la possibile guerra sociale.

Oggi tutto l'interesse dei compagni viene puntualmente deviato in modo sempre più totalizzante, sui soli aspetti spettacolari e commerciabili, come lo spettacolo di una solidarietà evirata dai conflitti sociali, con la collaborazione anche da parte dei compagni che non condividono questo modo di operare. In questo tipo di iniziative non vi è nulla di inerente a quel che più di ogni altra cosa dovrebbe interessarci: le modalità di una propaganda anarchica rivoluzionaria tesa a sviluppare un'azione insurrezionalista.
Se siamo rimasti noi stessi, testardi più di prima, a lottare e sostenere, al di là di ogni repressione e criminalizzazione

quello che contro ogni compromesso abbiamo portato avanti sul piano rivoluzionario, con chiarezza e consapevolezza, perché dovremmo abbandonare questa strada proprio ora. Se esiste una teoria e una pratica rivoluzionaria ancora degna di questo nome, questo è l'anarchismo rivoluzionario. Se esiste uno spirito di rivolta dell'individuo, un desiderio di insorgenza per dar corso alla totale autoliberazione individuale e sociale, questo è quanto abbiamo e sosteniamo e portiamo avanti da sempre.

Noi non abbiamo bisogno di rifarci il "maquillage", né abbiamo da rinnegare nulla del nostro passato, se c'è qualcosa che ci rimproveriamo,è la nostra insufficienza mostrata quando ci siamo adagiati.
Oggi noi dobbiamo approfondire tutto,ma per poter far meglio di quanto fin qui c'è riuscito di fare è sempre sulla strada aperta e violenta della rivolta "esplosiva" e dello scontro sociale armato contro lo Stato, il capitale, la Chiesa e tutti i loro innumerevoli rappresentanti e servitori.

No, noi non chiudiamo gli occhi sulla realtà, né ci stordiamo e ci lasciamo incantare dalle prefiche di "Liber asinorum" a tal punto, da non riuscire a più a distinguere chi è il nemico (e i suoi dintorni), ciò che va facendo per rendersi più attraente, partecipativo e accettabile.
Non ci interessano le "minestre" riscaldate della critica-critica, né i bigotti ripetitori delle formule sonanti, quanto vaghe e fors'anco vane, sia tra gli spaccamonti funesti e superflui, quanto per i contemplativi e i salmodianti della teoria "insurrezionalista". Noi non abbiamo fiducia nelle chiacchiere, né ci interessano le battaglie cartacee, noi ci vogliamo confrontare unicamente sul terreno dell'agire e su quello ragioniamo, perché lì stanno sempre i nostri problemi veri, in quanto ineriscono il qui e ora dell'azione rivoluzionaria anarchica all'interno dei conflitti sociali in corso.
Noi non agiamo solo per distruggere il presente sistema

sociale, ma anche contro chi all'interno delle lotte intraprese mira a creare nuove autorità e nuovi istituti di coercizione sociale al posto di quelli annientati.

Noi agiamo per risvegliare la rivolta contro i capi che comandano, contro il gregge che ubbidisce, per affermare la libera autonomia individuale,responsabile solo di fronte alla propria coscienza, il rispetto della sovranità del singolo di fronte alla stupida ed eunuca concordia pecorile delle masse, sempre prone agli ordini di vecchi e nuovi capi.
L'anarchia che incendia i nostri cervelli e infiamma i nostri cuori è inestinguibile fonte di entusiastico palpito rivoluzionario,che ci porta a voler abbattere iconoclasticamente tutte le divinità del cielo e della terra che albergano nella conservatrice e statica mentalità umana.
Siamo dei perfetti nichilisti e individualisti perché anarchici, e siamo anarchici perché amiamo la libertà e la solidale acrazia tra gli uomini. Saremo e resteremo ancora, forse, degli incompresi e saremo forse maledetti, calunniati, derisi; ma avremo l'orgoglio e la gioia serena, ragionata, convinta, cosciente, così facendo di aver dato sempre tutto per ciò che fa di un uomo un uomo, ossia vivere nell'orizzontalità della vita sulla strada degli uomini liberi.

"L'Esplosione – foglio anarco-nichilista di corrispondenze sovversivo-insurrezionali", Gennaio 2001, Anno 0, n° 0

TOR GUERRILLA MAIL (VIA TOR)

http://grrmailb3fxpjbwm.onion/

Su grrmailb3fxpjbwm.onion

TorGuerrillaMail ti fornisce un indirizzo e-mail usa e getta. Non è necessario registrarsi, è sufficiente visitare TorGuerrillaMail e verrà fornito un indirizzo casuale. Puoi anche scegliere il tuo indirizzo.

Puoi fornire il tuo indirizzo e-mail a chiunque non conosci. Puoi visualizzare l'e-mail su TorGuerrillaMail, fare clic su un collegamento di conferma, quindi eliminarlo. Ogni futuro spam inviato all'e-mail usa e getta verrà eliminato da TorGuerrillaMail, non raggiungendo mai la tua casella di posta, mantenendo la tua casella di posta sicura e pulita.

Consulta le domande frequenti di seguito per maggiori dettagli sul funzionamento della nostra e-mail temporanea.

http://grrmailb3fxpjbwm.onion/about

VAGANDO TRA ROVINE NASCOSTE

Vago tra rovine nascoste
Attraverso notti di veglia senza fine.
Io non appartengo a nessun luogo,
e nessuna epoca
Vivo nel passato e nel presente

Bandito dal tempo,
Sono un ombra senza era,
Ho in me la forza oscura,
Per non ascendere,
Per rimanere nel profondo
Dell’inumano,
A cui appartengo …sono il Misantropo
Per essere il maestro,
Non il servo.
Verso il limite
Verso un limite
Tornando nel rifugio
In cui le candele si accendono
I muri scritti di sangue …
L’abisso si riapre …sono il Misantropo
E il male è libero
Ancora una volta…
Gli anni diventano secondi,
I secondi diventano anni,
Il sangue diventa fuoco,
Il fuoco diventa sangue,
L’oscurità diventa luce,
La luce diventa oscurità,
Divento tutto,
Divento nulla,
Niente è casuale.
Tutto ha uno scopo.
Tutto ha un significato.
Come gli spiriti indomabili,
Erro, non appartengo a nessun luogo e non ho tempo.