

PRIVACY

RIVELAZIONI
ESCLUSIVE

La crittoanalisi di
enigma
portata a termine
da un genio

— PAGINA 7

Cosa c'entrano
i bitcoins con il
bruteforce
Gpu?

— PAGINA 11

Lo strumento
del nsa
che ci controlla

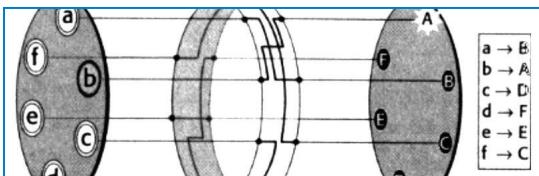
— PAGINA 13

La Privacy ormai è solo un sogno!

“I want to leave my footprints on the sand of time”

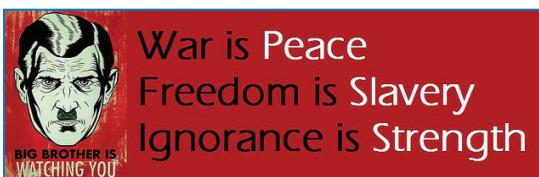


5

**Storia**

Digital enigma machine, E se vi dicesse che la vecchia Enigma è tornata alla ribalta con i suoi quattro cilindri?

7

**Italiano**

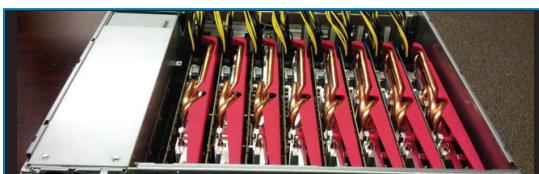
George Orwell 1984, Quello che Orwell scrisse nel 1948 è una previsione di quello che sta accadendo ora?

8

**Sistemi di Reti**

Gsm Spoofing, Siamo davvero sicuri che nessuno possa controllarci e che tutto è crittografato a dovere?

10

**Tpi**

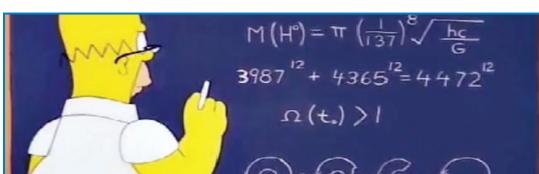
Sistemi di Bruteforce Gpu, Le Gpu compiono teraflop di calcoli al secondo ma per cosa altro le possiamo usare?

12

**Informatica**

I database ed I Metadati, E se vi dicesse che tutto quello che siamo è contenuto in un gigantesco database?

14

**Matematica**

Integrali Definiti, Perchè sono così importanti nella comunicazione cellulare Gsm?

16

**Gestione Progettazione Azienda**

Documentazione di progetto: gsm, Come è nata l'idea del Gsm Spoofing e come è stato progettato il metodo?

18

**ME**

Daniele Maisto, Chi è, da dove viene, cosa vuole fare e dove vuole andare?

Electronic Enigma Machine



Un po' di storia

La macchina Enigma fu sviluppata da Arthur Scherbius in varie versioni. La prima versione misurava appena $34 \times 28 \times 15$ cm³ ma aveva un peso vicino ai 12 kg, questo per via dei suoi pesanti componenti realizzati in acciaio.

Nel 1923 fu messa in vendita dello stesso Scherbius.

Sebbene i critogrammi prodotti dalla macchina fossero effettivamente indecifrabiili per l'epoca, molti commercianti e uomini d'affari pensarono che la possibilità di avere messaggi sicuri

non giustificasse l'alto costo della macchina. Dopo la prima guerra mondiale, le comunicazioni navali dei tedeschi erano state decriptate dalla Gran Bretagna, grazie anche

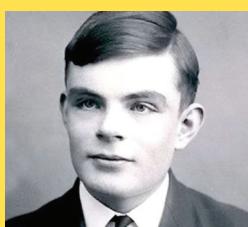
ai codici recuperati dopo l'affondamento di un incrociatore tedesco, il governo tedesco pensò di affidarsi a un sistema più sicuro per criptare i propri messaggi importanti.

Scherbius realizzò quindi una versione diversa dalla precedente, con i circuiti degli scambiatori modificati per impedire una decodifica dei messaggi nel caso che qualcuna delle macchine già in circolazione fosse caduta in mani nemiche.



Diversi esemplari furono acquistati dalla Marina Militare tedesca nel 1926, precisamente i modelli M4, poi nel 1929 il dispositivo venne acquisito dall'Esercito e da allora in poi praticamente da ogni organizzazione militare tedesca e dalla maggior parte della gerarchia nazista.

Uno dei primi modelli a tre cilindri



Alan Turing

Il genio che decifrò Enigma

"Possiamo vedere solo poco davanti a noi, ma possiamo vedere tante cose che bisogna fare"

Alan Turing un visionario il cui lavoro ebbe vasta influenza nel settore dell'informatica a quei tempi ancora poco sviluppata. È solitamente considerato il padre della scienza informatica e dell'intelligenza artificiale, da lui teorizzate già negli anni trenta.

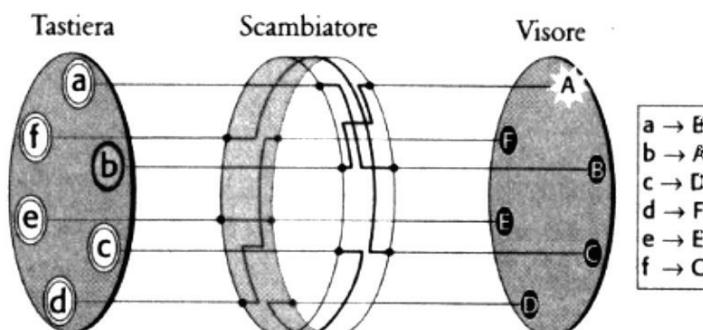
Egli fu anche uno dei più brillanti crittoanalisti che operavano in Inghilterra, durante la seconda guerra mondiale, Turing lavorò infatti a Bletchley Park, il principale centro di crittoanalisi del

Regno Unito, dove ideò una serie di tecniche per violare i cifrari tedeschi, incluso il metodo della Bomba (The Bomb) che già venne teorizzato da Rejewski, una macchina elettromeccanica in grado di decodificare codici creati mediante la macchina Enigma. Questo perché i due si accorsero di un dettaglio durante la fase di criptazione che poteva permettere attraverso un metodo a forza bruta di risalire alla combinazione di partenza dei cilindri.

Ma come funzionava Enigma?

M-Enigma (1923)

La versione base consisteva in tre componenti collegati da fili elettrici: una tastiera per immettere le lettere del testo in chiaro; un'unità scambiatrice che cifra la lettera trasformandola nel corrispondente elemento del crittogramma; e un visore con varie lampadine, che accendendosi indicano la lettera da inserire nel crittogramma. Il passo successivo dell'idea di Scherbius consiste nel far ruotare automaticamente il disco scambiatore di un sesto di giro (o di un ventiseiesimo di giro nel caso di un alfabeto completo di 26 lettere) dopo la cifratura di ogni lettera. I circuiti interni dello scambiatore determinano il modo in cui un elemento del testo chiaro è crittato. Con lo schema di base nella tabella di conversione è possibile realizzare in sostanza una semplice cifratura per sostituzione monoalfabetica ovvero una cifratura in cui ciascuna lettera è sostituita con un'altra. Ma Scherbius non si limitò solo a questo, aggiunse anche un pannello frontale chiamato plug-board con il quale gli operatori potevano effettuare un altro scambio, ancora prima che il segnale elettrico partito dalla tastiera arrivasse nello scambiatore.



Uno schema di enigma con alfabeto semplificato

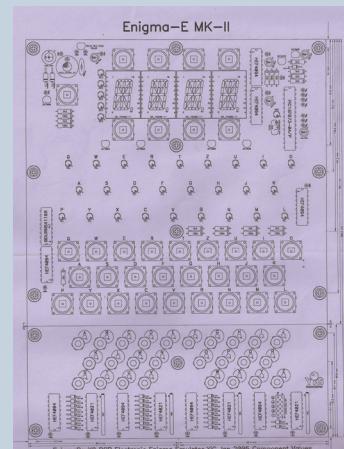
L'enigma continua...

E-Enigma (2017)

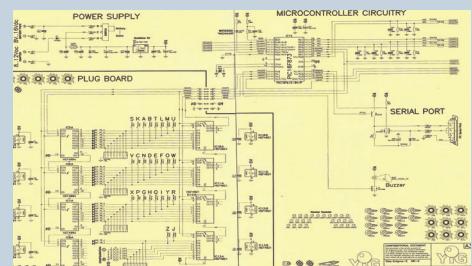
La versione elettronica consiste in vari componenti elettronici, tra quelli fondamentali abbiamo un PIC16F873 per dare una logica "informatica" alla macchina, dei Bit Shift Register HEF4021 usati come encoder per permettere al pic di controllare tutto, e un display a segmenti per settare la macchina. La macchina funziona in modo identico a quella di Scherbius ovviamente non usa rotori scambiatori meccanici troppo difficili e dispendiosi da costruire, ma un codice caricato su di un pic che li simula. È possibile selezionare il tipo di macchina M3 o M4 (rispettivamente tre e quattro cilindri). La cifratura avviene nello stesso modo di quella tradizionale ovvero inserendo come prima cosa la sequenza degli scambiatori e il tipo di riflettore, l'operatore ha la possibilità, digitando sulla tastiera una lettera, di vedere la stessa crittografata tramite un sistema di led collegati al Pic il quale si occuperà degli scambi. Il display è anche capace di mostrare le operazioni svolte dal pic per commutare la lettera in modo da essere ancora più chiaro l'algoritmo crittografico. La macchina è anche dotata di una porta seriale rendendola così in grado di connettersi ad una RPI così da implementare in futuro anche una turing BOMB.

Enigma: Versione Elettronica della macchina.

Una macchina che di meccanico oramai non ha più nulla, un pic che controlla tutta la logica degli encoder che codificano le informazioni, un mucchio di resistenze e almeno un centinaio di condensatori tutto alimentato da una batteria di 9 volts. Questa la E-enigma machine!

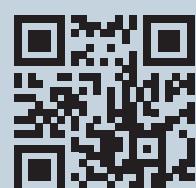


Uno dei progetti dell'E-Enigma



Lo schema elettrico dell'E-Enigma

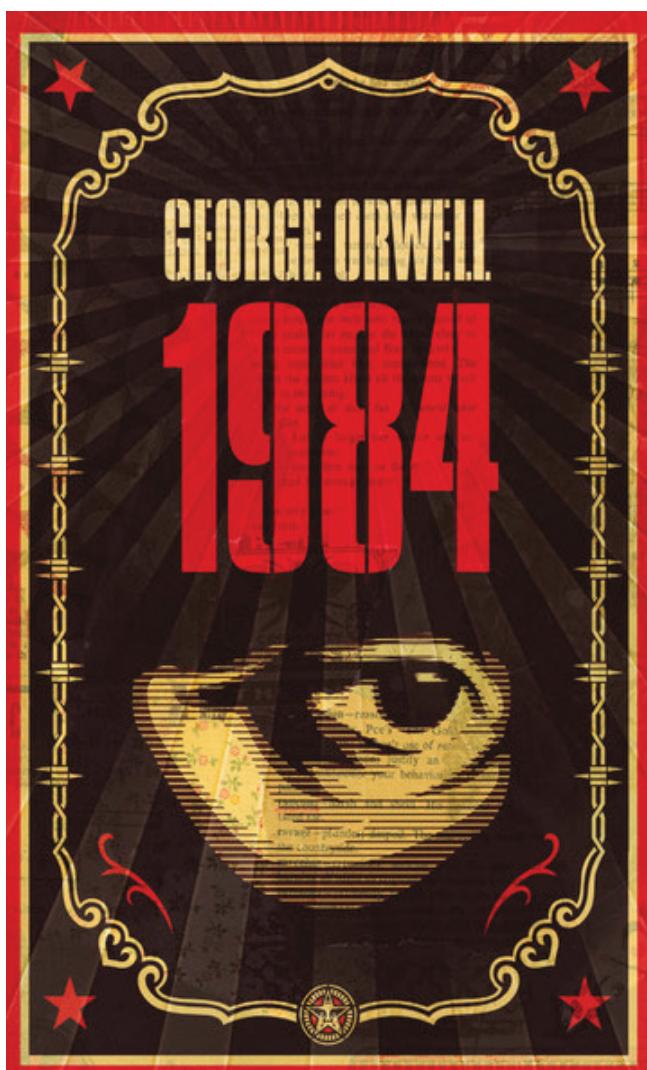
Guarda
l'assemblaggio
step by step del
E-Enigma



1984

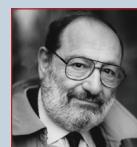
Abbiamo già visto tutto?

Il romanzo di George Orwell



Umberto Eco

ORWELL, O dell' energia visionaria.



Quasi per caso decise d'intitolare il suo romanzo *Nineteen Eighty-Four*. Pare avesse preso in considerazione anche il 1980 e il 1982 e si dice che alla fine la data sia venuta fuori invertendo quella del 1948, in cui egli stese l'ultima versione del romanzo. Orwell stava cercando un futuro abbastanza vicino per soddisfare i timori che realmente lo agitavano, e cioè che qualcosa di simile dovesse realmente accadere prima o poi. Ma per quanto casuale sia stata la scelta della data, anche il caso, una volta prodotto un evento, instaura una necessità: giunti al fatidico 1984 non possiamo ormai sottrarci ai fantasmi che questa data evoca. Essi fanno parte del nostro immaginario collettivo.

“La guerra è pace, la libertà è schiavitù, l'ignoranza è forza.”

“Finché non diverranno coscienti della loro forza, non si ribelleranno e, finché non si ribelleranno, non diverranno coscienti della loro forza.”

“Nulla vi apparteneva, se non quei pochi centimetri cubi che avevate dentro il cranio.”

“Il partito vi diceva che non dovevate credere né ai vostri occhi né alle vostre orecchie, e voi ascoltavate.”

Come Funziona il Gsm?

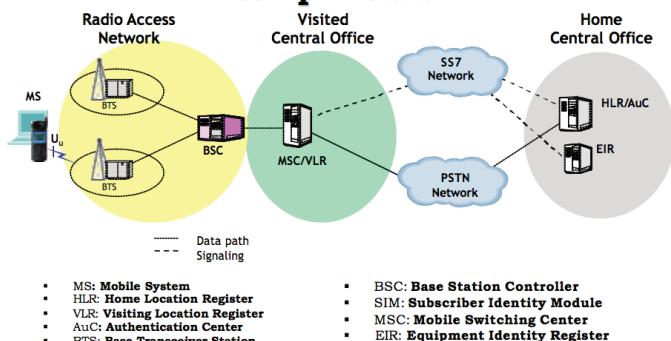
Mobile station (MS) - La stazione mobile è il dispositivo in grado di accedere alla rete GSM tramite il segnale radio. La stazione mobile può essere suddivisa in due parti separate; l'hardware mobile e la scheda SIM.

Base Station (BS) - È l'antenna che viene chiamata anche "cella". Una BS copre una particolare area cellulare della rete cellulare detta cella. La dimensione di questa cella può variare da poche centinaia di metri a diversi chilometri. Questo dipende anche dalle caratteristiche del paesaggio e dalla densità di popolazione dell'area. Nelle stazioni della metropolitana e negli edifici di grandi dimensioni, le stazioni di relay possono essere posizionate per agire come ripetitori. Queste stazioni poi collegano il segnale alla BTS più vicina.

Base Station Controller (BSC) - Questo controller controlla diverse bts. Gestisce i passaggi di sessione tra le diverse bts quando un utente si sta muovendo attraverso diverse celle. Se le stazioni di base non sono collegate allo stesso BSC, il trasferimento viene gestito dal MSC.

Mobile Switching Center (MSC) e Visitor Location Register (VLR) - Il centro di commutazione

GSM: architettura di riferimento semplificata



Sistema MSS - BSS - NSS

mobile è responsabile della gestione dell'autenticazione, del passaggio agli altri BSC e delle chiamate verso la rete fissa. Per raggiungere questo obiettivo, il MSC si basa sui quattro diversi database: HLR, VLR, AUC e EIR. Ogni MSC possiede un proprio registro dei visitatori (VLR). Il VLR detiene informazioni sugli abbonati degli abbonati che sono sotto la cura di MSC (che vengono copiati dal Registro di localizzazione locale (HLR)). Il VLR, ad esempio, detiene l'identità di sottoscrizione mobile temporanea (TMSI), che è un alias temporaneo per l'IMSI. Ciò significa ridurre la trasmissione frequente dell'IMSI.

Home Location Register (HLR) - Il HLR memorizza le informazioni personali dell'utente come l'IMSI e il numero di telefono. C'è solo un HLR per ogni provider di rete GSM.

Authentication Center (AUC) - Esso gestisce il processo di autenticazione di un abbonato alla rete. Più in particolare, l'AUC detiene la chiave segreta condivisa e genera una chiave casuale che viene utilizzata per l'autenticazione.

Equipment Identity Register (EIR) - Esso detiene i numeri di identificazione internazionale delle apparecchiature mobili (IMEI) di telefoni bloccati o rubati. Un numero IMEI è un numero unico assegnato a ogni telefono cellulare.

L'autenticazione tra Ms e BTS avviene tramite una chiave segreta condivisa: In altre parole usando la crittografia a chiave simmetrica. Questa chiave condivisa (Ki) viene memorizzata nella scheda SIM e nel Centro di autenticazione.

L'autenticazione procede come segue:

- 1) Come prima cosa l'MS manda le sue aspettative di sicurezza al VLR.
- 2) IL VLR manda una richiesta di identità al MS.
- 3) L'MS risponde con il suo codice IMSI.
- 4) Quando il VLR riceve l'IMSI, manda una richiesta AV (Authentication Vector) al AUC . L'AUC svolge i seguenti passaggi:
 - a) Genera 128-bit di numeri random (RAND)
 - b) Associa la RAND con la chiave segreta (Ki) che appartiene a questo IMSI.
 - c) Il RAND firmato viene quindi utilizzato per creare una risposta corrispondente a 32 bit (SRES) e una chiave di sessione a 64 bit (Kc).
 - d) Spedisce l'IMSI, RAND, SRES e Kc al VLR.
- 5) Il VLR invia quindi la RAND (non firmata) alla MS
- 6) L'MS firma questa RAND con la chiave segreta (Ki). Se il Ki è lo stesso del Ki memorizzato sull'AUC, allora dovrebbe generare esattamente lo stesso SRES.
- 7) L'MS invia la sua versione del SRES.
- 8) Il VLR controlla quindi se SRES == SRES. Se lo sono, allora l'autenticazione è riuscita.
- 9) Il VLR assegna un TMSI per ridurre i pacchetti dell'IMSI in trasmissione sulla rete.
- 10) Il VLR invia anche la chiave Kc (sessione) al BS.

How does Gsm spoofing work?

Tutto si basa su una scheda rtl-sdr, adattata con un software chiamato Yate che fa quello che dovrebbe fare una bts ovviamente manca ancora l' NSS che viene emulato da YateBts (N.I.B.) un altro software che comprende il Gmsc e il Vlr. Ma soffermiamoci un attimo sulle vulnerabilità che abbiamo sfruttato per costruire questa rogue Bts. Si basa sul sistema di autenticazione con cui avviene la connessione tra BTS e MS. Questa infatti si basa su un protocollo di autenticazione non mutuo: la rete autentica MS, ma l'MS non autentica la rete. Oltre a questa anche un'altra la vulnerabilità che possiamo sfruttare, ciò è quella di attacco passivo attraverso lo sniffing (lo sniffare pacchetti gsm), con un semplice device di poche decine di euro infatti possiamo implementare un sistema di sniffing gsm che catturi i dati su di una determinata frequenza poi essendo gli stessi crittografati come abbiamo visto in precedenza necessitano di una decodifica, poiché usano un cifrario A5/1 basta un semplice programmino Kraken che occupa solo un po' di risorse (circa 2TB di rainbowtable precalcolate per il cracking GSM). Nella mia versione dell'attacco uso una rogue bts che si sostituisce alla bts standard attraverso un processo di man in the middle facendo credere all' MS di essere la BTS Leggittima.

Gpu hash cracking

Perchè usare una Gpu al posto di una Cpu? Semplice! Anche se nelle attuali Cpu esiste il calcolo parallelo, esso è molto difficile da implementare ma soprattutto da ottimizzare per ottenere le stesse performance di una Gpu. Mentre in una normale Scheda grafica è tutto molto più semplice grazie alla sua struttura hardware, completamente diversa da quella Cpu. Basti pensare che ad oggi si contano più di un milione e mezzo di software che usano Cuda come sistema di calcolo parallelo e che gran parte di questi software sono anche 100 volte più efficienti dello stesso implementato su una Cpu. Una Cpu i9 Serie X esegue 1 teraflop di operazioni al secondo mentre una Gpu Nvidia tesla arriva fino a 20 teraflop di operazioni al secondo. Questo anche perchè le Gpu hanno un numero di core nettamente maggiore di una Cpu.

Ma cosa c'entra tutto questo con il bruteforce ?



Una GPU ha molti core (centinaia). Ogni nucleo è fondamentalmente in grado di calcolare un'operazione aritmetica a 32 bit per ogni ciclo di clock. Infatti, la GPU funziona bene con il parallelismo estremo: quando ci sono molti processi di lavoro identici da eseguire ("identici", cioè "stesse istruzioni", ma non "stessi dati"). Alcuni dettagli, per una vecchia scheda NVidia (un GTX 9800+, dell'inizio del 2009): in essa ci sono 128 core, suddivisi in unità multicore da 16. Ogni multicore può avviare 8 operazioni per ciclo di clock (da cui l'idea di 128 core è 16 volte 8). Il multicore gestisce le unità di lavoro ("thread") per gruppi di 32, in modo che quando un multicore disponga di un'istruzione da eseguire, effettua effettivamente quell'istruzione sui suoi 8 core su 4 cicli di clock. Si tratta dell'avvio dell'operazione: ogni singola operazione richiede fino a 22 cicli di clock. Potete immaginare l'istruzione ed i suoi operandi come un'onda in una piscina: una data onda richiede un

certo tempo per raggiungere l'altra estremità della piscina, ma è possibile inviare diverse onde in sequenza. Quindi è possibile mantenere il ritmo di "128 operazioni a 32 bit per ciclo" solo fino a quando si hanno almeno 22 volte il numero di "thread" da eseguire (cioè un minimo di $22 \cdot 128 = 2816$), in modo tale che i thread possano essere raggruppati in pacchetti di 32 "identici" che eseguono le stesse istruzioni allo stesso tempo, come i ballerini di hip-hop. Un hardware più recente sarà più veloce, ma le GPU dominano comunque. Un PC host, sulla sua CPU (un quad core 2.4 GHz Intel Core2), potrebbe raggiungere circa 48 milioni di SHA-1 al secondo, questo con un codice ottimizzato SSE2. Un singolo hash utilizzerà circa 500 cicli di clock su una tale CPU (la CPU può calcolare diverse istruzioni in un singolo ciclo, a condizione che non competono per le risorse e non dipendono l'uno dall'altro) a 2400 MHz, quindi 48 milioni al secondo. Con un'implementazione SHA-1, ma un GTX 9800+ e il clock GPU di 1450 MHz, per un totale complessivo di circa 160 milioni di computazioni SHA-1 al secondo.

Cosa centra il Bitcoin Mining con questo?

Nel mondo dei bitcoin il mining è il modo utilizzato dal sistema e dalle criptovalute in generale per emettere moneta. La rete bitcoin memorizza le transazioni all'interno di strutture di dati chiamate in gergo "blocchi". Affinchè un blocco possa essere aggiunto alla catena dei blocchi, ovvero all'enorme database pubblico contenente tutte le transazioni in bitcoin, è necessario che un elaboratore lo "chiuda" trovando un particolare codice, che può essere unicamente azzeccato a furia di tentativi (Bruteforce). Questa operazione cristallizza il blocco, impedendo qualsiasi modifica futura, e chi trova tale codice è ricompensato con una certa quantità di bitcoin (attualmente 25), più tutte le tasse delle transazioni da lui inserite nel blocco, come incentivo alla "donazione" di tempo macchina alla causa del bitcoin. Per questa operazione fino a due anni fa venivano utilizzate gpu in cluster data la loro enorme potenza computazionale adesso si usano gli ASIC (microprocessori costruiti su misura per un preciso compito).

Guarda uno sketch di
comparazione tra
GPU e CPU



I bigdata e XKeyScore

Facile da usare come Google ma con una potenza di calcolo e un database 100 volte superiore.

Secondo una presentazione di diapositive del 2013 fatta dal Nsa Xkeyscore è un “Sistema di Sfruttamento DNI / Analytic Framework”. I DNI sono quegli strumenti che sfruttano la

Digital Network Intelligence ciò è l'intelligenza derivata dal traffico internet. Ad esempio il valutare ricerche su Google da parte di specifici individui o masse di individui.

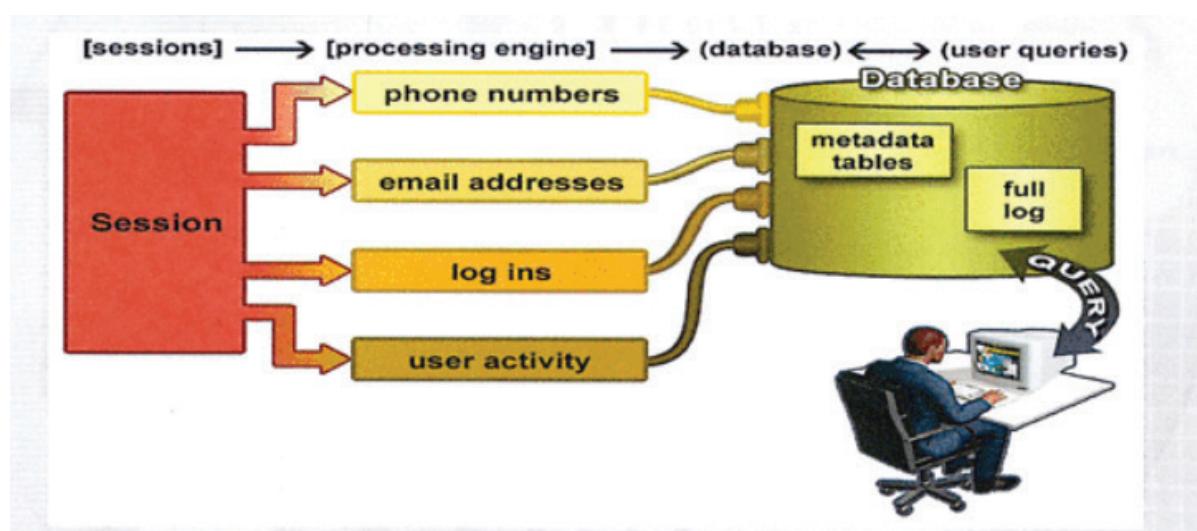
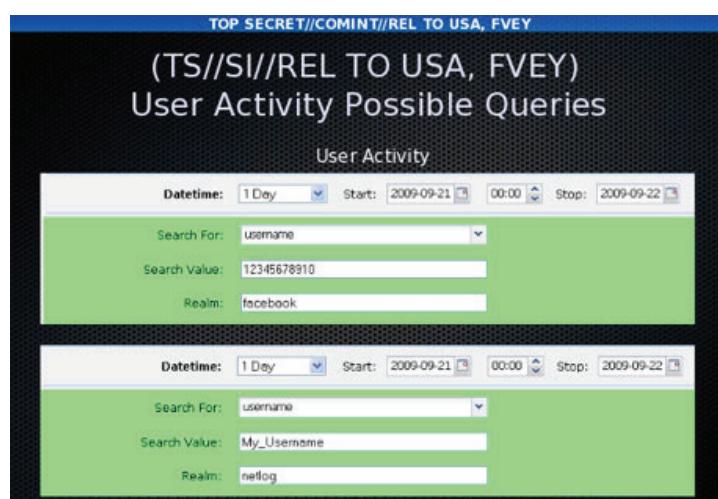
Edward Snowden parla di XKeyscore come un motore di ricerca front end”.

XKeyscore è una sorta di software per creare query, nelle quali ci sono i metadati descrittivi che fungono da chiave di ricerca per l'interrogazione del database. I metadati

servono per l'identificazione ed il recupero degli oggetti digitali, sono costituiti da descrizioni dei documenti fonte o dei documenti nati in formato digitale.

Le caratteristiche di XKeyScore e la sua semplicità permettono agli analisti dell' Nsa di cercare attraverso i metadati qualsiasi cosa come email, telefonate o semplici cronologie di browser web. Associati ovviamente all'individuo o al gruppo di individui target. Gli analisti possono infatti cercare, attraverso il nome, il numero di telefono o anche secondo parole chiavi specifiche proprio come un vero e proprio motore di ricerca. E non è finita qui:

tutte queste informazioni potevano essere richieste senza alcuna autorizzazione.



Ma quanto ci controlla l'NSA

Non hai bisogno di parlare con terroristi per sospettare che le tue comunicazioni vengano analizzate dall'NSA

L'agenzia è infatti abilitata a navigare in tre "hops" dal suo target iniziale, persone che parlano con persone che parlano con te (amici di amici), persone che parlano con persone che parlano con persone che parlano con te (amici di amici di amici).

Quindi il tipico utente che ha 200 amici, avrà 32.680 amici di amici, approssimativamente il numero dei corpi studenti della Columbia University e 5.339.912 amici di amici di amici approssimativamente più della popolazione del Minnesota, tutti controllati dall'NsA.

Number of friends:

[Login to Facebook](#)



200

or more than the capacity of a
Concorde



ACTUAL: 100



32,680

or more than the Columbia University
student body



ACTUAL: 28,824



5,339,912

or more than the population of
Minnesota



ACTUAL: 5,303,925

**Edward
Snowden**



"Quanto siete disposti a sacrificare della vostra vita privata per il beneficio di uno stato di sorveglianza globale?"

Quando ero seduto alla mia scrivania e lavoravo ogni giorno con strumenti di sorveglianza di massa, ho potuto osservare come tutte le nostre comunicazioni venissero intercettate quotidianamente in assenza di qualsiasi sospetto di irregolarità. E questo accadeva a nostra insaputa, senza il nostro consenso. I documenti, hanno stabilito che la sorveglianza di massa, la sorveglianza delle popolazioni non solo di individui sospetti, è qualcosa che si verifica sempre e costantemente... Uno dovrebbe potersi fidare di agenzie per la sicurezza che hanno potenziale accesso completo ai dettagli della nostra vita. Sono stato fedele ai ruoli e agli obblighi del mio giuramento (...)

Immersion, il tool del MIT

Il mit ha creato uno strumento utile per capire quali sono i metadati persenti nella nostra mail. Basta infatti autorizzare il proprio account e, nel giro di pochi secondi, si potranno visualizzare tutta una serie di informazioni sul nostro conto: le persone con cui scambiamo più messaggi, i network di cui fa parte ogni nostro contatto, il volume di email in entrata e in uscita negli anni, chi ha introdotto per la prima volta un contatto, i "collaboratori" con cui si hanno più conversazioni e via dicendo. Anche senza accedere ai contenuti, "i metadati possono tracciare un profilo molto chiaro sulla nostra personalità", ha commentato

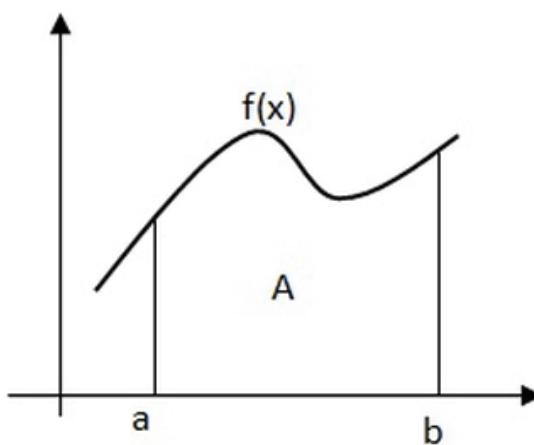
Ethan Zuckerman, direttore del MIT Media Lab.

"Quando visualizzi il network dei tuoi contatti (...) inizi a capire che non interagisci solo con la persona con cui scambi l'email, ma con una ragnatela di individui, ognuno dei quali è connesso ad altri attraverso decine o centinaia di percorsi indiretti che esistono anche in tua assenza", ha spiegato al Boston Globe César Hidalgo, uno dei tre ideatori del tool. Questo ancora una volta ci fa riflettere sull'enorme mole di dati personali che sono presenti in rete e su come essi possano essere usati per capire chi siamo.

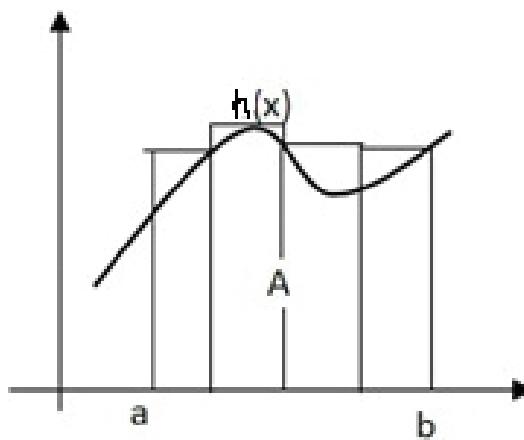
Gli integrali definiti

Nel gsm gli integrali definiti sono utilissimi come in qualsiasi altro tipo di comunicazione analogica o con portante analogica, perché grazie a loro possiamo calcolare l'area di figure piane curvilinee.

Data una funzione $f(x)$, l'integrale definito in un certo intervallo $[a,b]$ ha un significato geometrico preciso: rappresenta l'area A compresa tra il grafico della funzione $f(x)$, l'asse x e le due rette verticali $x=a$ e $x=b$.



La definizione rigorosa di integrale (dell'integrale di Riemann) considera le possibili approssimazioni per eccesso (o per difetto) dell'area A , effettuate con funzioni a gradino costruite al di sopra (o al di sotto) della curva. Esistono infinite funzioni a gradino: ecco per esempio il disegno di una funzione di questo tipo che approssima A per eccesso.



Se la migliore approssimazione per difetto e per eccesso coincidono, diremo che tale numero è il valore dell'integrale definito della funzione, cioè dell'area A .

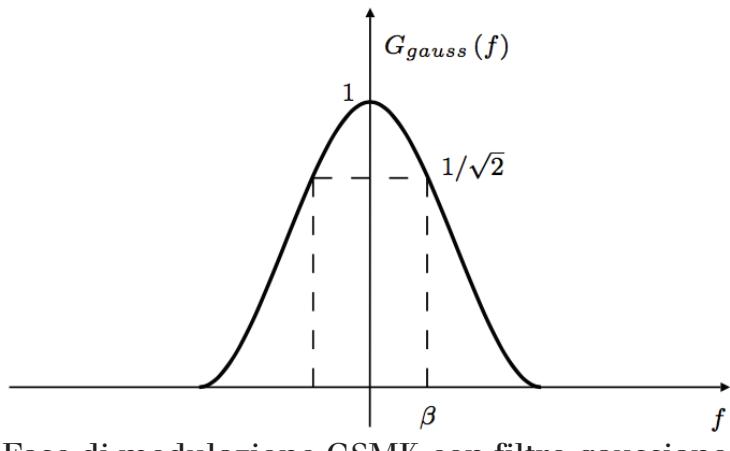
Nella pratica, il procedimento per trovare l'area A non tiene conto di tutte queste sottigliezze tecniche; Esiste infatti il teorema fondamentale del calcolo integrale, che ci permette di calcolare il valore dell'integrale definito seguendo questo procedimento:

- Trovare una primitiva di $f(x)$, cioè una funzione $F(x)$ tale che $F'(x) = f(x)$;
 - Calcolare $F(a)$ e $F(b)$
 - Sfruttare il teorema, che afferma questo:

$$A = \int_a^b f(x)dx = F(b) - F(a)$$

Cosa c'entra con il gsm?

La ragione risiede nel fatto che, per ottenere una maggiore efficienza energetica, gli amplificatori delle MS devono necessariamente lavorare nella zona di saturazione e quindi in regime non-lineare.

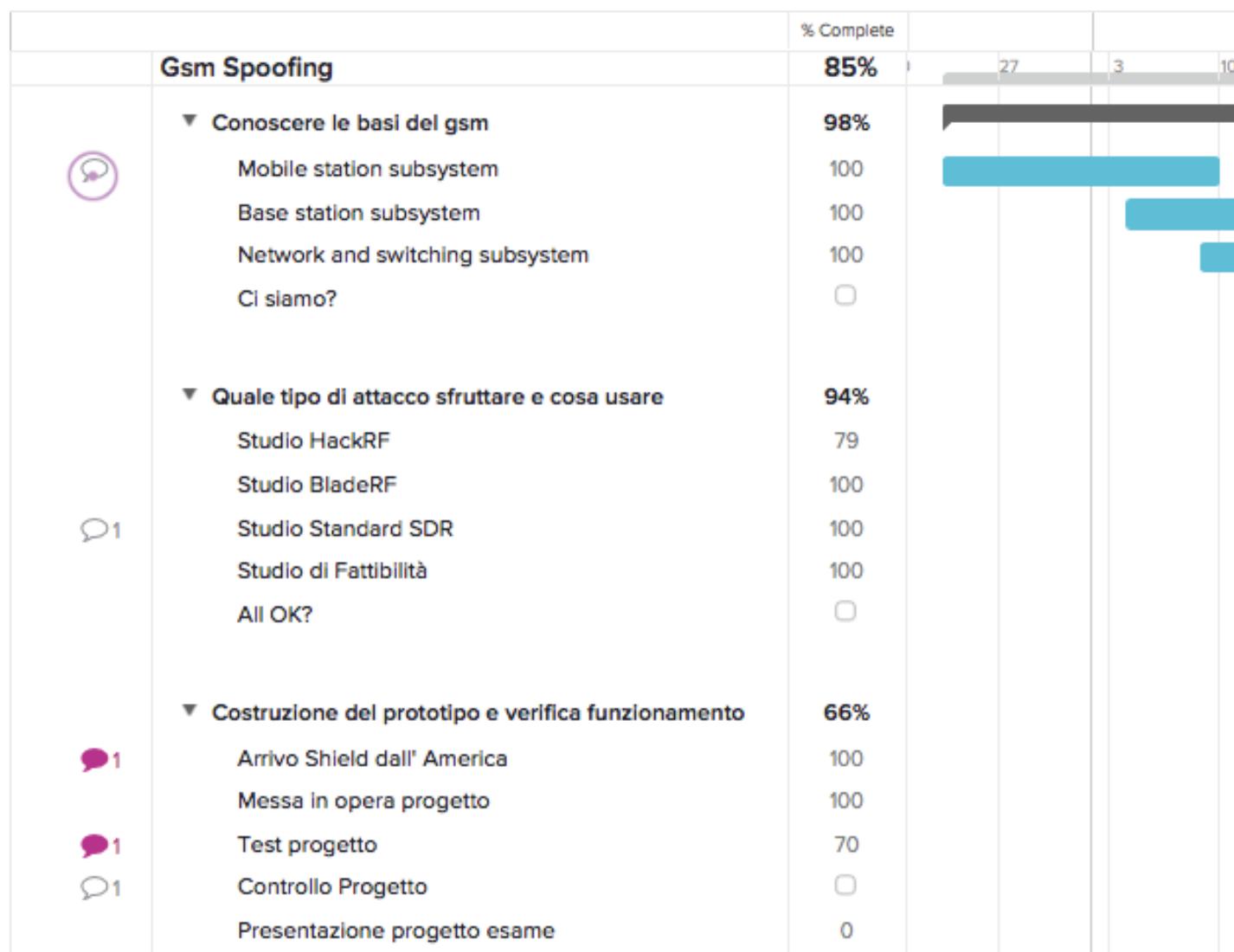


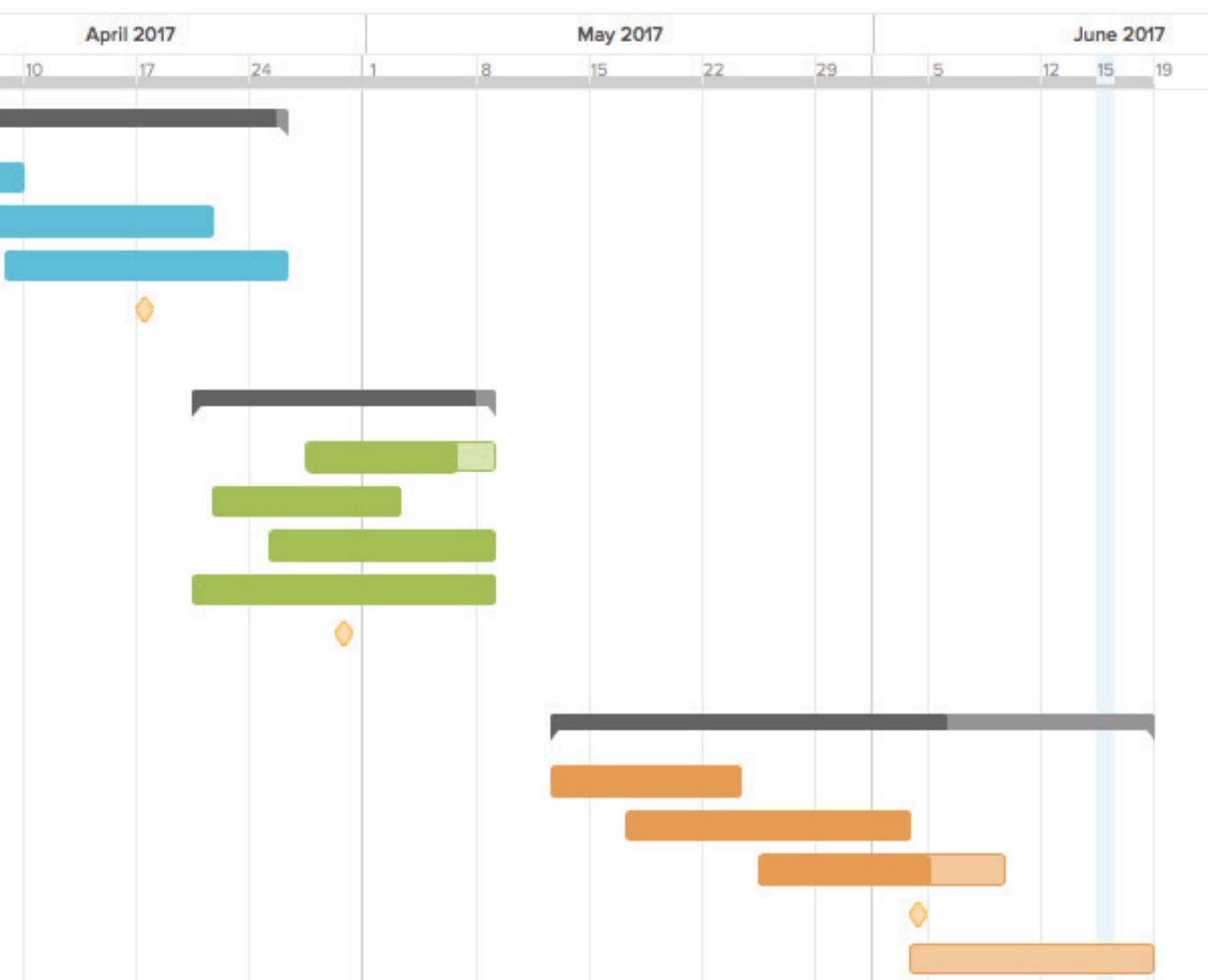
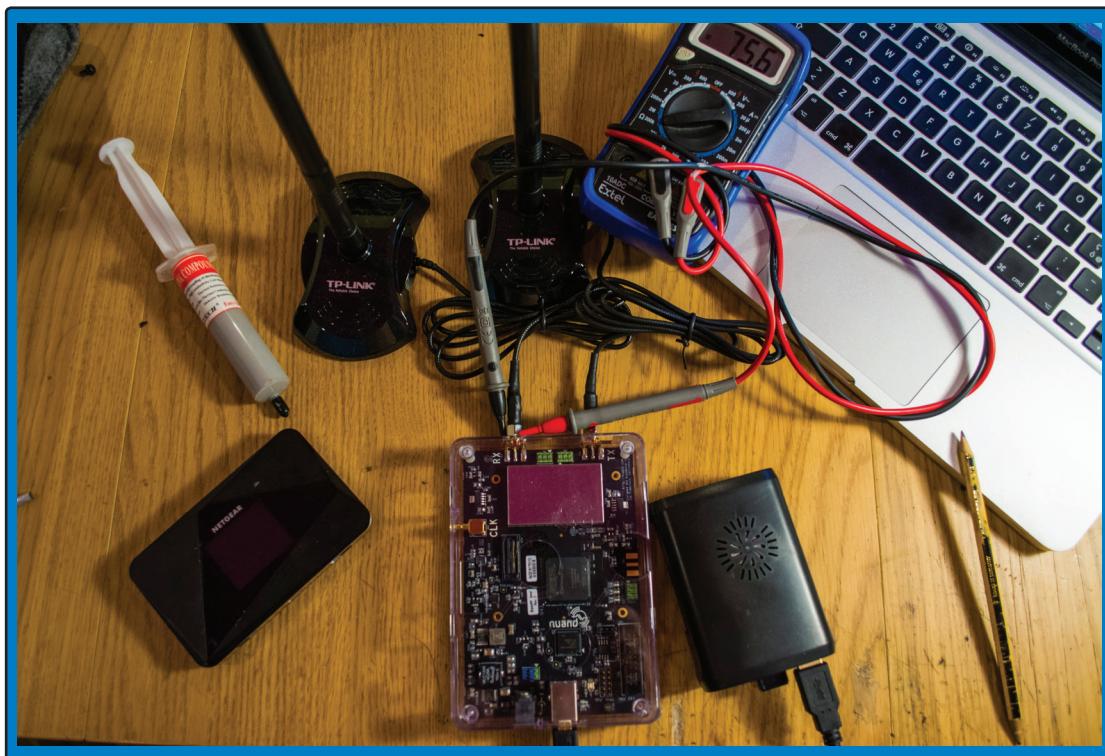
Fase di modulazione GMSK con filtro gaussiano

Introducendo un filtro gaussiano come quello sopra mostrato, l'effetto che abbiamo è quello di ottenere uno spettro di potenza del segnale in uscita al modulatore FM sensibilmente più compatto rispetto ai classici segnali MSK(Gsm classico). In particolare, lo spettro GMSK presenta lobi secondari notevolmente più ridotti e consente quindi una spaziatura assai serrata dei canali, rispettando le severe norme di emissione fuori banda stabilite dalle specifiche GSM.

Come siamo arrivati al Gsm spoofing?

Mi ha sempre affascinato il mondo delle comunicazioni, il gsm è sempre stato vulnerabile dalla sua nascita. La sinergia tra queste due cose mi ha portato a costruire un network Gsm proprio, con una sua BTS e un suo NSS sul quale qualsiasi persona ignara potesse conettersi senza notare nulla. Sia chiaro niente di tutto questo è stato fatto per nuocere qualcuno, tutto è a semplice scopo illustrativo e dimostrativo di quanto sia semplice e redditizio un Gsm Spoofing.





Connecting the dots.

Ho un iphone, un ipad e un mac ma non ho mai seguito Steve Jobs. Ho sempre pensato che le sue ricchezze si basassero sullo sfruttamento dei bambini e su quello delle persone. Un giorno in classe la prof di inglese ci fece ascoltare il discorso di Steve alla Stanford University: diceva tante cose interessanti ma una è rimasta stampata nella mia mente, "collegare i puntini". Si perchè Jobs parlava di una serie di eventi scollegati che

poi alla fine hanno portato al suo esordio. Avrei tantissime storie da raccontarvi su come l'unire i puntini nella mia vita mi ha portato a conquiste inaspettate nonostante la mia giovanissima età.

Ma preferisco che i fatti parlino per me.

Chi sono?

Sono Daniele, ho 19 anni vivo a Napoli, frequento il 5^o anno al Galileo Ferraris di Scampia, ho conquistato insieme al mio team il 200^o posto nella classifica del Google #code. In secondo superiore ho "hackerato" il sito della scuola perchè il tecnico che lo aveva creato aveva garantito diritti superuser a tutti ed infatti cambiando solo la richiesta nel get riuscivo a mettermi un bel dieci in informatica che da lì in poi è diventato un must. Ho creato anche

un programmino in visual basic che lo faceva da solo così chiunque poteva usufruirne tutto questo, ovviamente, con un amico più pazzo di me. Lavoro in una emittente televisiva e mi occupo delle reti e dei sistemi trasmissivi ad esse collegati. Quando non ho nulla da fare faccio penetration testing su reti in giro e non ci crederete ma 9 su 10 hanno ancora la password admin e l'altro 1% non sa cambiare quella dell'SSH.

“ Sono le persone che nessuno immagina che possano fare certe cose, quelle che fanno cose che nessuno può immaginare “

Il vostro dovere è non accontentarvi e pensare l'impossibile.



Dicono di me

Giovanni Russo

Editore TeleclubItalia

Daniele l'ho conosciuto per caso. Lavoravamo ai Fratelli Maristi e lui pensò di darci una mano per capire cosa facevamo. Daniele è così. Ama la scoperta. Ama capire. Ama conoscere. Qualsiasi cosa abbia un funzionamento in poco tempo non è più un mistero per lui. Tutti noi siamo circondati da oggetti di cui ignoriamo le più semplici regole, lui no. Lui non chiede, studia. Lui non impara, approfondisce. Negli anni è anche cambiato. Prima era timido ed introverso ora invece sta divenendo sempre più un uomo. Riservato, educato e gentile ma con molti meno timori del domani. La sua capacità di essere sempre pronto a confrontarsi con le cose lo ha reso un punto fermo della nostra squadra. Gli piace stare con noi ed a noi piace stare con lui. Io lo chiamo il mio Golden Boy perché Daniele è un ragazzo d'oro che potrà fare della vita ciò che vuole anche se nella vita non ci sono tutorial che ti accompagneranno, ci saremo sempre noi al tuo fianco.

Fabio Lamonea

Communication Designer / The Club Factory Advertising

Di Daniele amo il suo saper mettere il cuore in quello in cui crede, quello che fa, nel rapporto con le persone che lo circondano. Quando qualcosa scuote la sua curiosità deve approfondirla e deve portarla avanti con tutte le sue forze. Il risultato dello studio poi può non essere sempre positivo o fruttuoso ma una cosa è sicura e costante: il cuore che ci mette.

Andrea Setaro

Regista & Responsabile Tecnico TeleclubItalia

Ho incontrato Daniele su un set mentre giravamo uno spot per una scuola media, lui dava una mano alla scuola dove era cresciuto. Aveva 16 anni. Mi sono reso subito conto che aveva una scintilla. Una scintilla chiamata passione. Passione e curiosità per tutto quello che vedeva. Tutto ciò che non sapeva lo approfondiva, lo studiava, si preparava. Molti suoi coetanei sono appiattiti sull'effimero, lui no. Daniele dopo ormai 3 anni che lo conosco è diventato un punto di riferimento nella nostra crew, la sua voglia di scoprire, la sua educazione, la sua intelligenza e le sue capacità lo porteranno a realizzare tutto ciò che vorrà. Perchè se esiste un problema Daniele lo saprà risolvere!

Pasquale Rosiello

Video-Maker TeleclubItalia

Una persona merita la mia stima quando è sempre disponibile, merita la mia stima quando sa sempre dare una risposta alle mie domande, quando sa ridere e sa farti ridere, quando è generosa, merita la mia stima quando sa stare allo scherzo, sono poche le persone che hanno tutta la mia stima una di queste è Daniele perchè queste caratteristiche le possiede tutte!

Alessia Paccagnella

Studente Politecnico di Milano

Daniele è un ragazzo che ama mettersi in gioco in ogni situazione, nonostante la sua timidezza, e che non si lascia mai sfuggire le opportunità di imparare qualcosa di nuovo. Vinta la sua personalità introversa, riesce a trovare una buona sinergia con le persone riuscendo così a lavorare bene in gruppo.

È infine un buon amico, generoso e che tiene alle persone a cui vuole bene alle quali è sempre disponibile a regalare il suo tempo.

Carlo Turrioni

Ingegnere Meccanico

Ho incontrato Daniele nell'ambito di un progetto ambizioso, da subito ho colto il suo entusiasmo nel fare le cose, s'interessa praticamente di tutto e per questo puoi averlo al tuo fianco per affrontare qualsiasi problema di natura tecnica, informatica, elettrica o elettronica; non disdegna per questo le materie umanistiche, come la psicologia o l'antropologia insomma un personaggio con mille sfaccettature destinato a grandi cose, un diamante grezzo che deve solo trovare la giusta concentrazione per brillare.

Questo magazine è stato prodotto interamente da Daniele Maisto per l'esame di stato 2017, il suddetto è pubblico e cedibile
ogni sua copia è liberamente disponibile

in rete sotto MiT License.

dmrecords.eu

Revisione Testi / Mariarosaria Ferrara

Revisione Grafica / Fabio Lamonea