Introduzione alla crittografia ed alla crittoanalisi

di Enrico Zimuel

Italian Cyberspace Law Conference 2001
Bologna 29 Novembre 2001

Che cos'è la crittografia?

- La **crittografia** (dal greco *kryptos*, nascosto, e *graphein*, scrivere) è la scienza che si occupa dello studio delle scritture "segrete".
- E' nata come **branca della matematica e dell'informatica** grazie all'utilizzo di tecniche di teoria dei numeri e di teoria dell'informazione.
- E' entrata a far parte della nostra vita quotidiana per la **protezione delle informazioni digitali**. Dalle smart card, ai cellulari, alle trasmissioni via Internet, alle tv satellitari, etc.

Orgini storiche

- La **crittografia** è una scienza antichissima nelle società primitive qualunque tipo di scrittura è di per sé “magico” e “segreto”.
- La **scitala lacedemonica** è un antico esempio di un sistema per cifrare messaggi tramite l’utilizzo di un bastone cilindrico (secondo gli scritti di Plutarco, in uso dai tempi di Licurgo, IX sec a.C.).
- Medioevo, con **Gabriele Lavinde** (che scrisse un manuale nel 1379, conservato ancora in Vaticano), in Francia all’epoca del cardinale Richelieu con **Antonio Rossignol** e soprattutto in Italia con **L.B.Alberti, G.B.Porta, G.B.Bellaso, G.Cardano**.

Orgini storiche

- All'inizio del secolo durante la prima guerra mondiale con il generale **Luigi Sacco**, dell'esercito italiano, che scrisse il famoso "Nozioni di crittografia" (1925).
- Il periodo d'oro della crittologia è senza alcun dubbio quello della seconda guerra mondiale quando **Alan Turing**, il padre dell'informatica teorica, insieme al gruppo di ricerca del Bletchley Park formalizzò la matematica necessaria per uno studio sistematico dei cifrari.
- **Claude Shannon**, l'ideatore della moderna teoria dell'informazione, che nel 1949 pubblicò un articolo rimasto nella storia "Communication theory of secrecy systems".

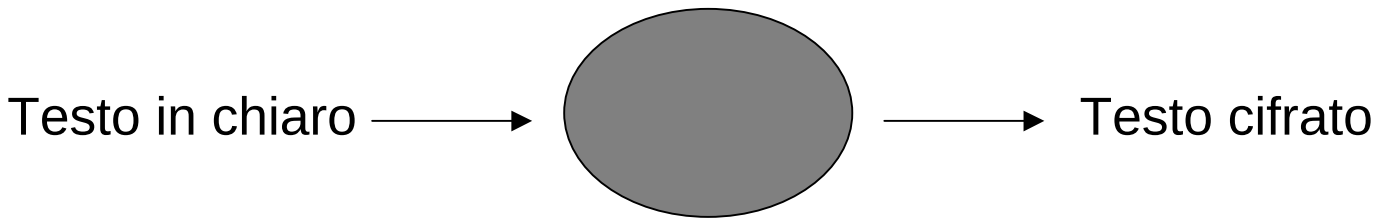
Orgini storiche

- **Enigma** la più famosa macchina crittografica della seconda guerra mondiale.

- Nasce in Inghilterra il primo elaboratore elettronico il **Colossus** utilizzato per decifrare le comunicazioni “segrete” dei nemici.

Le basi della crittografia

- Per **sistema crittografico** si intende un sistema in grado di cifrare e decifrare un messaggio attraverso l'uso di un algoritmo (metodo di calcolo) e di una chiave (una stringa segreta alfanumerica).
- Il messaggio che dovrà essere cifrato viene chiamato **testo in chiaro** (plaintext) mentre il risultato dell'algoritmo crittografico **testo cifrato** (ciphertext).



Sistema crittografico

Principio di Kerckhoffs

- Un principio fondamentale della crittologia moderna afferma che: *“La sicurezza di un crittosistema non deve dipendere dalla segretezza dell’algoritmo usato, ma solo dalla segretezza della chiave”*
- Pubblicato nel1883 nel libro “La criptographie militarie”
- Basti pensare che ormai quasi tutti gli algoritmi crittografici moderni, utilizzati nelle più disparate tecnologie, vengono rilasciati con i codici sorgenti.

Le basi della crittografia

- Fondamentalmente i sistemi crittografici si dividono in due tipologie:

Sistemi crittografici

Sistemi **simmetrici**

Si utilizza una sola chiave per cifrare e decifrare

Sistemi **asimmetrici**

Si utilizzano una coppia di chiavi:
una per cifrare
e l'altra per decifrare

I cifrari simmetrici

- Utilizzano la stessa chiave per cifrare (**encryption**) e decifrare (**decryption**) i messaggi.
- Hanno il problema della trasmissione della chiave tra mittente e destinatario.

I cifrari simmetrici

- Il classico esempio del cifrario di **Cesare**: si traslano i caratteri dell'alfabeto del testo in chiaro di 3 posizioni verso destra.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

- Ad esempio: il testo in chiaro "PROVA DI TRASMISSIONE" con il cifrario di Cesare diventa "SURBDGNZUDVPNVVNRQH".

I cifrari simmetrici

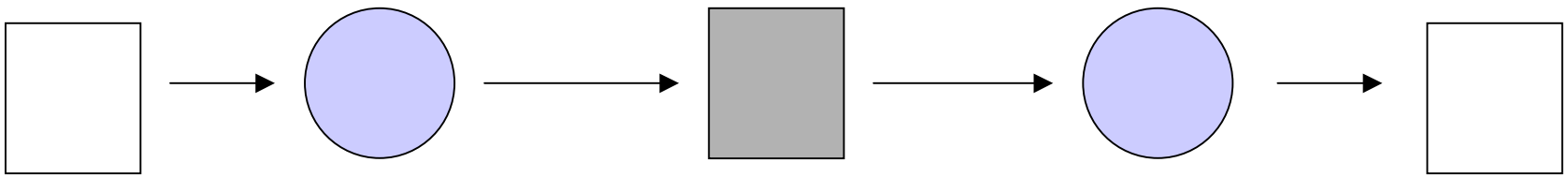
- Nella crittografia moderna vengono utilizzati molto nei sistemi ibridi per la loro velocità di elaborazione.
- I più conosciuti ed utilizzati cifrari simmetrici sono:
  - Feistel (1973)
  - DES (Data Encryption Standard, 1977), 3DES
  - IDEA (1991)
  - BlowFish (1993)
  - RC5 (1994)
  - CAST-128 (1997)
  - Rijndael (nel 2000 diventa AES, Advanced Encryption Standard)

I cifrari asimmetrici (a chiave pubblica)

- Di recente scoperta: 1976, da due ricercatori W.Diffie e M.Hellmann della Stanford University.
- Utilizzano una coppia di chiavi per le operazioni di encryption e decryption.
- Una chiave detta pubblica (**public key**) viene utilizzata per le operazioni di encryption.
- L'altra chiave, detta privata (**private key**), viene utilizzata per le operazioni di decryption.
- A differenza dei cifrari simmetrici non è più presente il problema della trasmissione delle chiavi.

I cifrari asimmetrici

- Esempio:



$K_{pu}B$ = chiave pubblica dell'utente B

$K_{pr}B$ = chiave privata dell'utente B

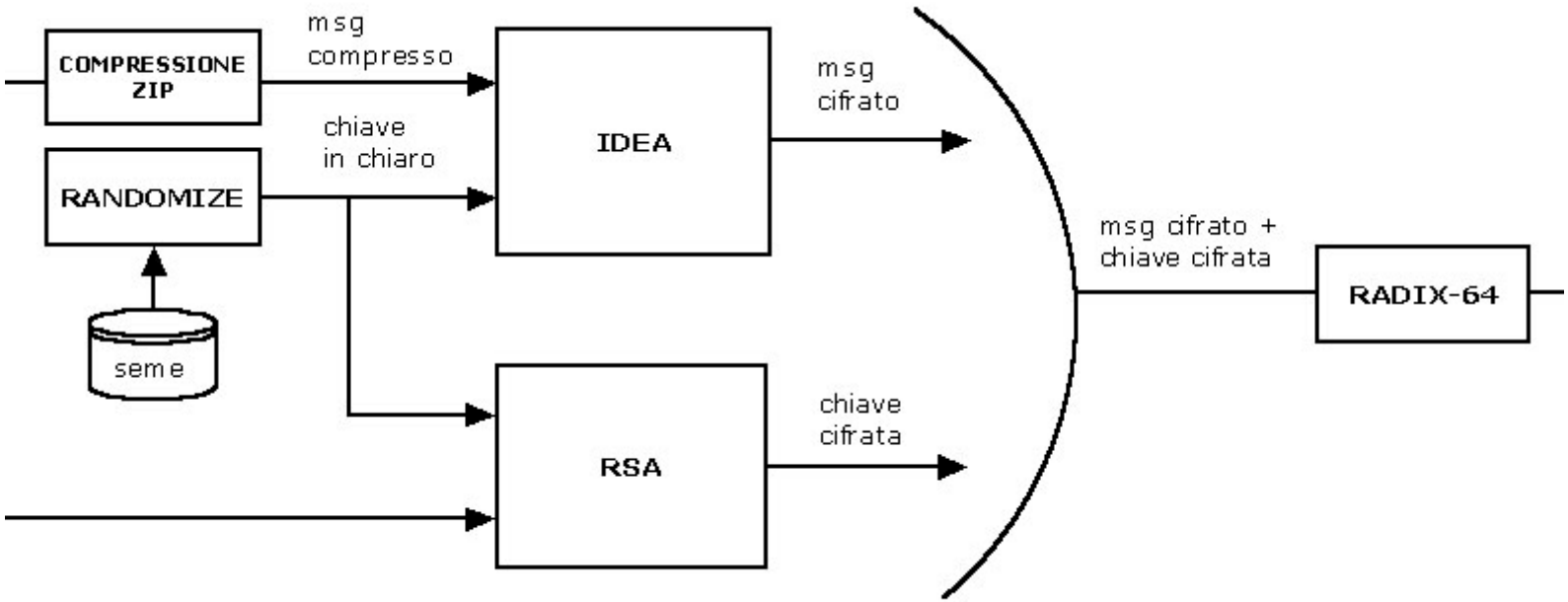
I cifrari asimmetrici (la nascita dei sistemi PKI)

- Dove trovo le chiavi pubbliche dei miei destinatari?
- Creazione di “archivi certificati” di chiavi pubbliche, i public key server.
- Ma chi mi garantisce la corrispondenza delle chiavi pubbliche con i legittimi proprietari?
- Nascita delle certification authority.
- A questo punto chi garantisce la rispondenza delle certification authority?
- Atto di fede!

I cifrari asimmetrici

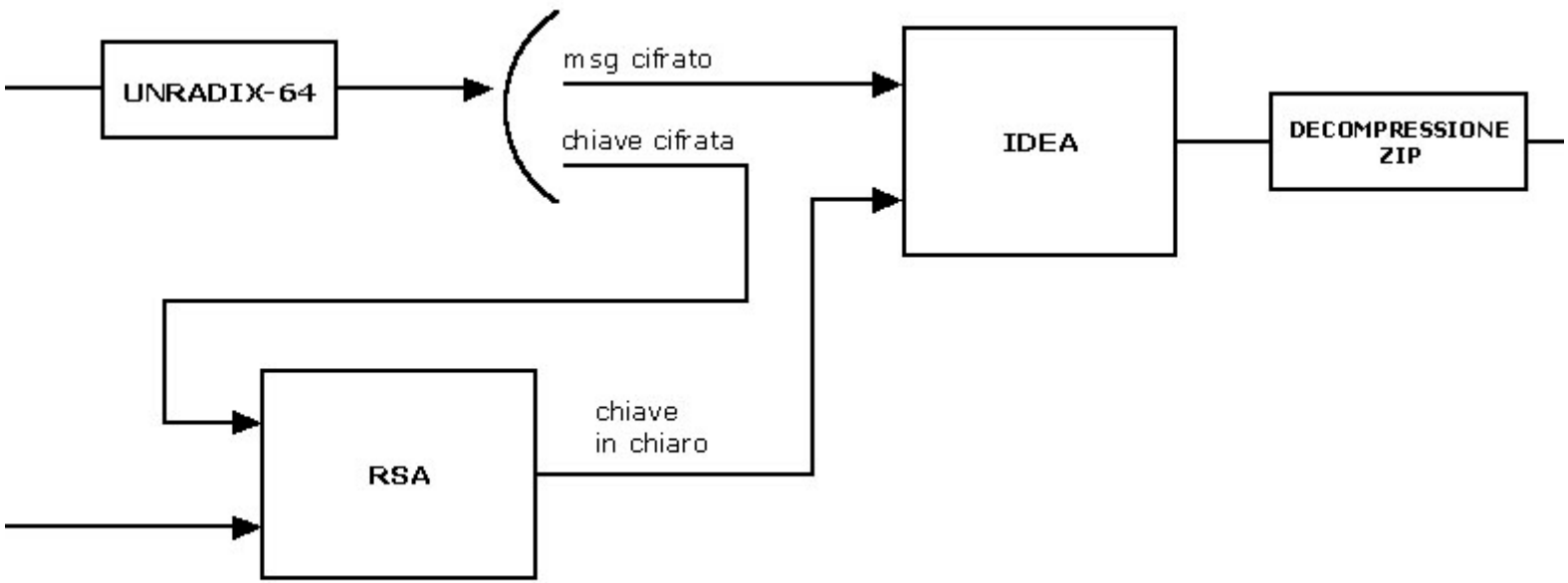
- Attualmente i più utilizzati cifrari asimmetrici sono:
  - RSA (1977, Ron Rivest, Adi Shamir, Len Adleman)
  - Diffie-Hellman
  - DSS (1991, FIPS PUB 186)
  - ECC (IEEE P1363, Crittografia delle curve ellittiche)

I sistemi ibridi, esempio di funzionamento del PGP



PGP (cifratura di un msg.)

I sistemi ibridi, esempio di funzionamento del PGP



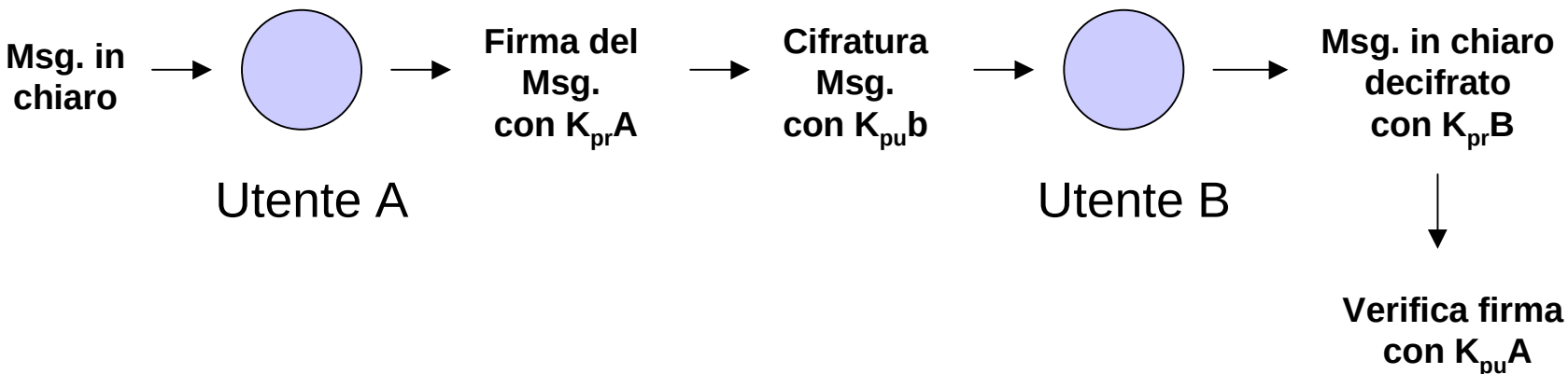
PGP (decifratura di un msg.)

La firma digitale

- Nasce come applicazione dei sistemi a chiave pubblica.
- Si utilizza la propria chiave privata per firmare un documento: in pratica viene generata una firma elettronica, una sequenza fissa di byte, una specie di “targa”, per un dato documento.
- Ad ogni documento diverso corrisponde una firma digitale diversa.
- Tecnicamente vengono utilizzate le funzioni hash one-way.
- Utilizzando le funzioni di encryption e di firma digitale in maniera combinata si ottiene la riservatezza e l’autenticazione.

Esempio di crittografia e firma digitale

- Esempio:



$K_{pu}A/B$ = chiave pubblica dell'utente A/B

$K_{pr}A/B$ = chiave privata dell'utente A/B

Le funzioni hash one-way

- Attualmente gli algoritmi più utilizzati sono:
  - MAC (Message Authentication Code)
  - HMAC
  - SHA-1 (1993, Secure Hash Algorithm)
  - MD5 (sviluppato da Ron Rivest)
  - RIPEMD-160 (per il progetto europeo RACE Integrity Primitives Evaluation)

La crittoanalisi

- La scienza che si occupa dell'analisi e della validità degli algoritmi crittografici.
- Analizzando il contenuto di un testo cifrato, attraverso tecniche statistico/matematiche si possono ottenere informazioni sul testo in chiaro.
- Per fortuna ciò non è sempre possibile, la maggior parte dei cifrari moderni è ancora al sicuro da tecniche di crittoanalisi.
- La storia ci insegna che non esistono cifrari inviolabili.

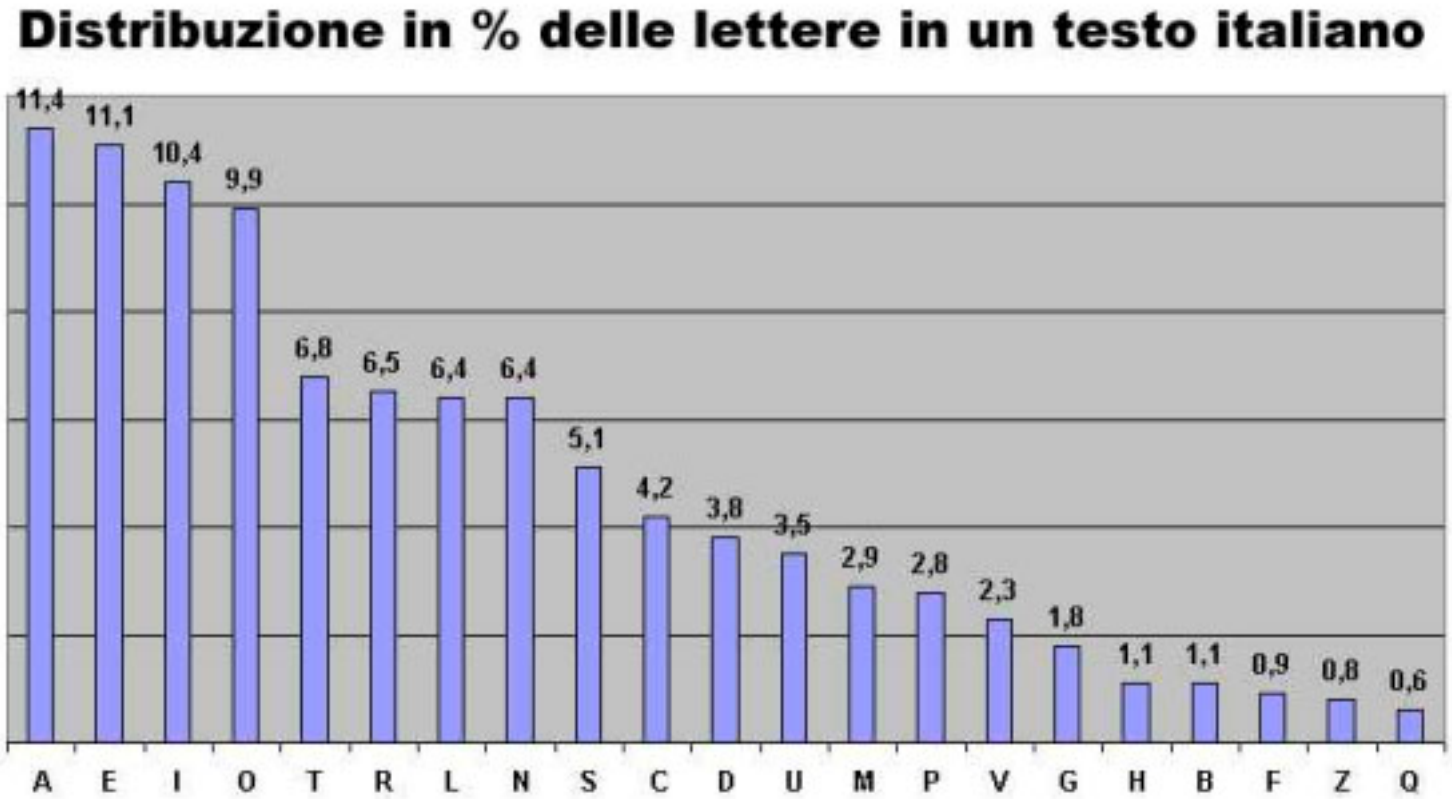
Le basi della crittoanalisi

- L'attacco ad un sistema crittografico ha l'obiettivo di forzare il sistema, il metodo scelto e il suo livello di pericolosità dipendono dalle informazioni in possesso del crittoanalista.
- Fondamentalmente esistono queste tipologie di attacchi:
  - Cipher Text Attack (il crittoanalista è in possesso di soli alcuni crittogrammi)
  - Known Plain-text Attack (il crittoanalista è venuto a conoscenza di una serie di testi in chiaro e di crittogrammi)
  - Chosen Plain-Text Attack (il crittoanalista ha scelto una serie di testi in chiaro e di crittogrammi)

La crittoanalisi statistica

- Tramite l'utilizzo di tecniche statistiche sulla frequenze dei caratteri o sottostringhe del testo cifrato si ottengono informazioni utili sul testo in chiaro.
- Ad esempio con il cifrario di Cesare effettuando una semplice analisi statistica delle lettere contenute nel testo cifrato e confrontando i risultati con le frequenze assolute dell'alfabeto della lingua italiana posso ricostruire il messaggio originale.

La crittoanalisi statistica



Esempio di crittoanalisi statistica del cifrario di Cesare

- Analizzando la frequenza delle lettere del testo cifrato “surbd gn zudvpnvvnrqh” ne escono i seguenti risultati: s (1/19), u (2/19), r (2/19), b (1/19), d (2/19), g (2/19), n (3/19), z (1/19), v (3/19), p (1/19), h (1/19).
- Le lettere con maggiore frequenza risultano essere la n e la v con frequenza 3/19 ed a seguire la u, la r, la d, la g con frequenza 2/19.
- Associo a queste lettere le più frequenti corrispondenti all’alfabeto italiano nel grafico visto in precedenza.
- Provando con la combinazione d=a, n=i, u=r, r=o si ottiene il seguente testo parzialmente decifrato: “s**ro**b**a** g**i** z**ra**vp**i**vv**io**qh” con una certa fantasia ed abilità linguistica (un po’ come avviene nei giochi di enigmistica o nei quiz televisivi alla Mike Buongiorno) già in questa frase si potrebbe ottenere il testo in chiaro “prova di trasmissione”.

Possibili tecniche di attacco

- **Brute-force**, ossia tramite il calcolo di tutte le possibili combinazioni di chiavi del cifrario. Con l'aumento della potenza di calcolo degli elaboratori questa tecnica banale stà diventando sempre più efficace. Basti pensare al Cracking del DES a 56 bit con un computer multiprocessore costruito dall'EFF in grado di violare l'algoritmo in poche ore di calcolo!
- **Crittoanalisi differenziale**, tramite l'analisi delle "distanze" numeriche dei caratteri presenti nel testo cifrato e l'ausilio di sofisticate tecniche matematiche unite ad algoritmi sempre più veloci.
- **Man-in-the-middle**, sfruttando il sistema delle infrastrutture PKI un eventuale intruso può posizionarsi tra un mittente ed un destinatario e scambiare le loro chiavi pubbliche e private con altre opportunamente modificate.

Esempio di attacco al formato OPENPGP

- E’ un attacco che sfrutta un bug sul formato aperto internazionale OPENPGP.
- Scoperto da due crittologi della Repubblica Ceca, Vlastimil Klima e Tomas Ros nel 2001.
- L’attacco scoperto sul formato OpenPGP è basato sul fatto che alcune informazioni "delicate" sulla chiave pubblica e privata di un utente non sono protette adeguatamente nel file di configurazione del programma crittografico che si sta utilizzando.
- Modificando queste informazioni con dei dati prestabiliti si possono ottenere dei valori numerici utilizzabili per il calcolo della chiave privata dell’utente.

La sicurezza della crittografia

- La sicurezza di un sistema crittografico è basato sulla robustezza dell'algoritmo.
- Le tecniche di crittoanalisi diventano sempre più sofisticate grazie anche all'aumento della potenza di calcolo dei computer.
- Solo con la condivisione delle informazioni e delle specifiche tecniche degli algoritmi crittografici si può ottenere sicurezza.
- La filosofia open source è di vitale importanza per il settore crittografico.
- La storia ci insegna che gli algoritmi segreti sono quelli più insicuri.
- Gli algoritmi crittografici più importanti ed utilizzati da tutti devono essere di pubblico dominio, non ci possiamo fidare delle "black box".
- Sicurezza = Trasparenza.

IL GNUPG, l'alternativa open source al PGP

- Il progetto tedesco GNUPG (GNU Privacy Guard) nasce nel 1997 per opera di Werner Koch, sviluppatore indipendente open source.
- L'obiettivo è la realizzazione di un engine crittografico aderente alle specifiche del formato OPENPGP.
- Piena compatibilità con PGP2
- Disponibile in più versioni: Gnu/Linux, Ms Windows, FreeBSD, OpenBSD, AIX, Sun Os, BSDI, IRIX, etc.
- Disponbili vari front-end per sistemi GUI: Gnome, KDE, Ms Windows, etc.
- Attualmente è disponibile la versione 1.0.6.

Bibliografia

- “Sicurezza delle reti - Applicazioni e standard” di William Stallings, Addison-Wesley Editore.
- “Crittografia - Principi, Algoritmi, Applicazioni” di P. Ferragina e F. Luccio, Bollati Boringhieri Editore.
- “Crittografia” di Andrea Sgarro, Franco Muzzio Editore.
- “Segreti, Spie e Codici Cifrati” di C.Giustozzi, A.Monti, E.Zimuel, Apogeo Editore.
- “Codici & Segreti” di Simon Singh, Rizzoli Editore.
- “Crittologia” di L. Berardi, A.Beutelspacher, FrancoAngeli Editore.
- “Sicurezza dei sistemi informatici” di M.Fugini, F.Maio, P.Plebani, Apogeo Editore.