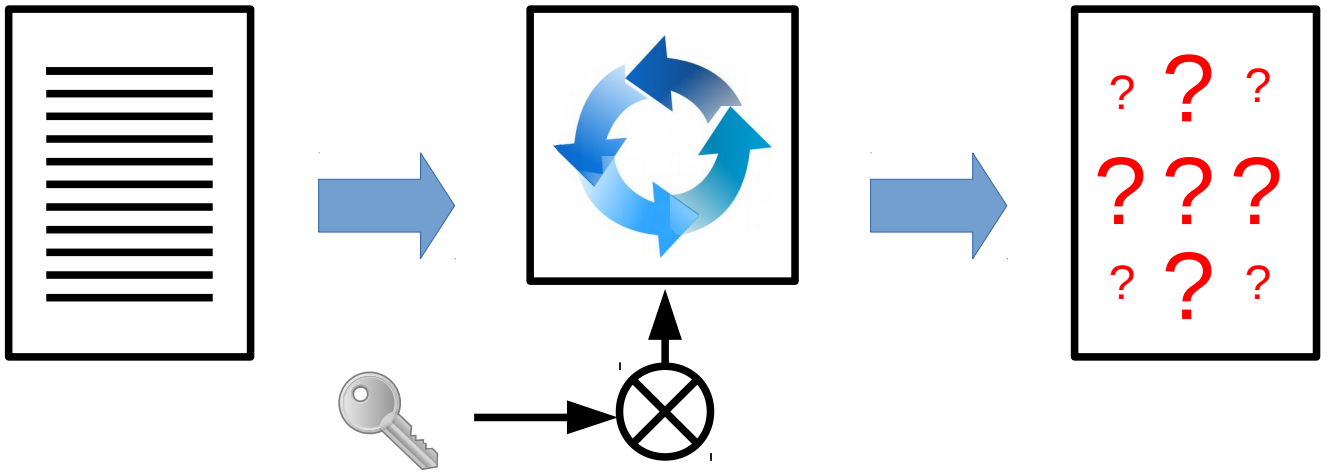
La Crittografia

Ing. Simone Giustetti

studiosg@giustetti.net

Definizione

- **SCRITTURA NASCOSTA**
- Scopo: **OFFUSCARE L'INFORMAZIONE**
- Rendere l'informazione accessibile solo a chi sia autorizzato a fruirne



Finalità

- Segretezza
- Privato
  - Privacy
  - Protezione dalle truffe
  - Protezione dalla pubblicità
- Lavorativo
  - Salvaguardia delle informazioni sensibili
  - Protezione della proprietà intellettuale
  - Contromisura allo spionaggio industriale

Principi della Crittografia - 1

Vincoli dell'operazione di cifratura:

- Non distruttiva

  Non deve causare perdita di informazione
- Reversibile

  Deve essere sempre possibile ricostruire l'informazione originale
- Sicurezza

  Deve essere indecifrabile

Minacce

- Aumento della **Velocità dei Collegamenti**
- Proliferazione di servizi on-line
  - E-commerce
  - Internet Banking
  - Servizi pubblici / pseudo pubblici
- Proliferazione di dispositivi collegabili in rete
  - Cellulari / Smart-phone
  - Sistemi di Sorveglianza
  - Tablet

Strumenti Istituzionali Inadeguati - 1

Soluzione con errori = Falsa sicurezza

E-mail

- Standard: Dati in chiaro
- SSL: Cifratura del traffico limitata alla comunicazione tra client / server
- Traffico server / server in chiaro
- Social Engineering

Strumenti Istituzionali Inadeguati - 2

Soluzione con errori = Falsa sicurezza

GSM

- Cifra solo il traffico tra dispositivo e cella
- Il traffico interno è in chiaro
- Il traffico non è tracciabile
- Gli algoritmi contengono errori
- Utilizza chiavi corte (64 o 128 bit)

Strumenti Istituzionali Inadeguati - 3

Soluzione con errori = Falsa sicurezza

Wi-Fi - 1

- WEP contiene falle, ma è l'unico protocollo supportato dalla totalità dei dispositivi
- WPA contiene falle e non era supportato da molti access point
  - Usa chiavi corte (64 o 128 bit)

Strumenti Istituzionali Inadeguati - 4

Soluzione con errori = Falsa sicurezza

Wi-Fi - 2

- WPA2 scoperte continuamente nuove falle.
  - Richiede aggiornamenti continui.
  - Giudicato sicuro con configurazione ad hoc e passphrase di lunghezza > 20 caratteri.
- WPA3 rilasciato Luglio 2018 e già accreditato di potenziali falle.

Strumenti Istituzionali Inadeguati – 5

Soluzione con errori = Falsa sicurezza

“Cloud”

- Il 97% dei 1.000 principali siti mondiali hanno subito almeno un furto di credenziali nel corso degli ultimi 10 anni.
- I furti sono tenuti nascosti fino a quando non diventa impossibile nascondere la verità.
- I sistemi di autenticazione centralizzati hanno peggiorato la situazione.

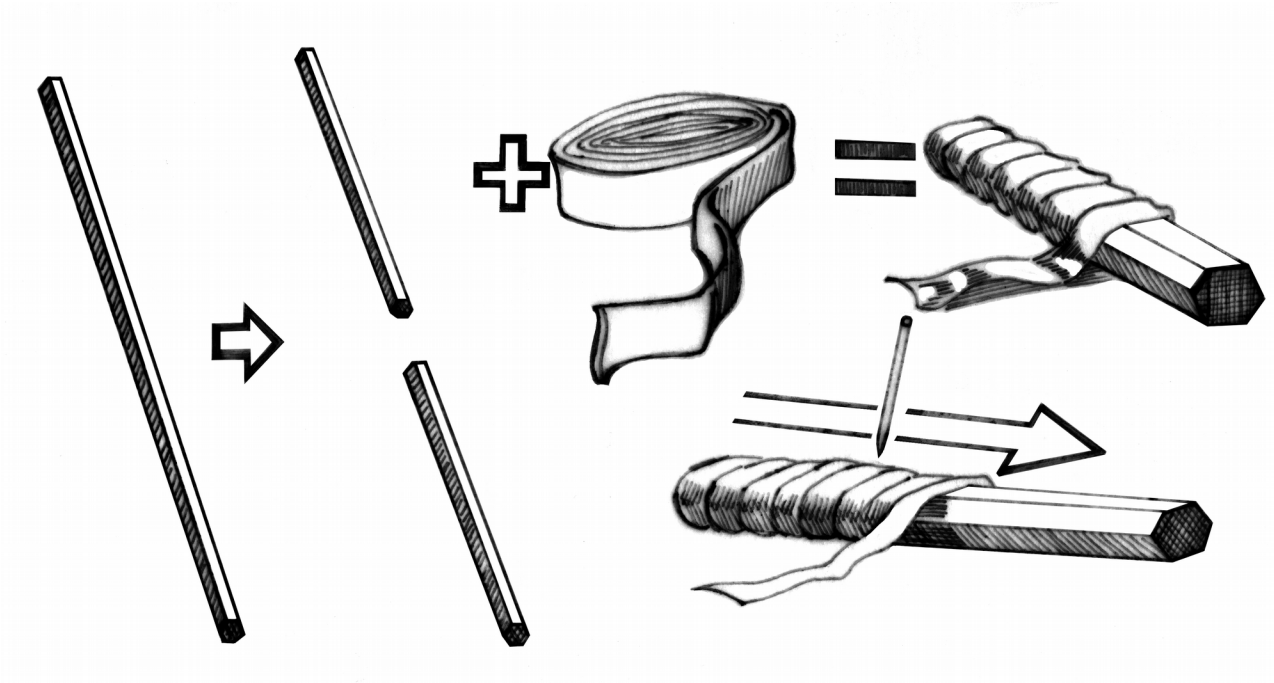
La Crittografia Limita i Danni

- La crittografia non previene intrusioni non autorizzate o furti di dati
- La crittografia impedisce la lettura delle informazioni agli intrusi ed ai ladri
- La crittografia non ha funzione di prevenzione, ma di limitazione dei danni
- I reali vantaggi sono apprezzabili solo in seguito ad un incidente e vengono spesso sottovalutati

Crittografia nella Storia - 1

- Notizie storiche di impiego nell'antico Egitto
- Grecia – 4° secolo AC

Bastone di Plutarco o Scitala Lacedemonica



Crittografia nella Storia - 2

- Grecia – 150 AC

Scacchiera di Polibio

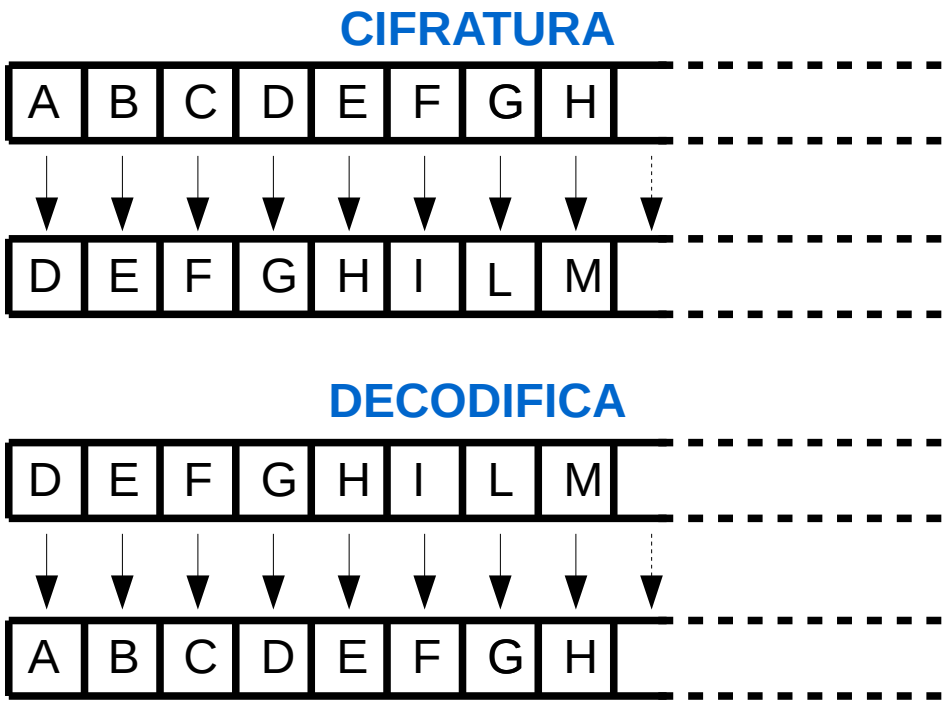
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

A = 11
B = 12
C = 13
...
X = 53
Y = 54
Z = 55

Crittografia nella Storia - 3

- Roma – 58 / 50 AC

Cifrario di Cesare



Tecniche di Attacco

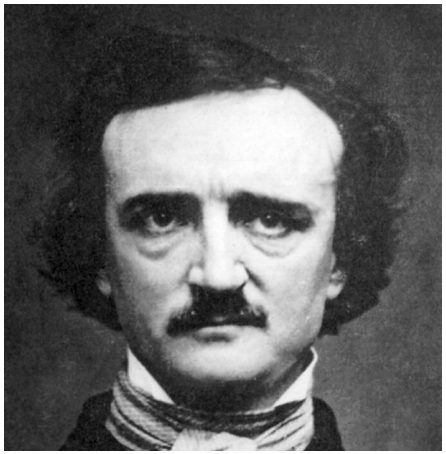
Le applicazioni della crittografia usate nel primo millennio DC sono passibili di Attacchi Statistici ossia di interpretazione basata sulla frequenza dei simboli nel documento cifrato

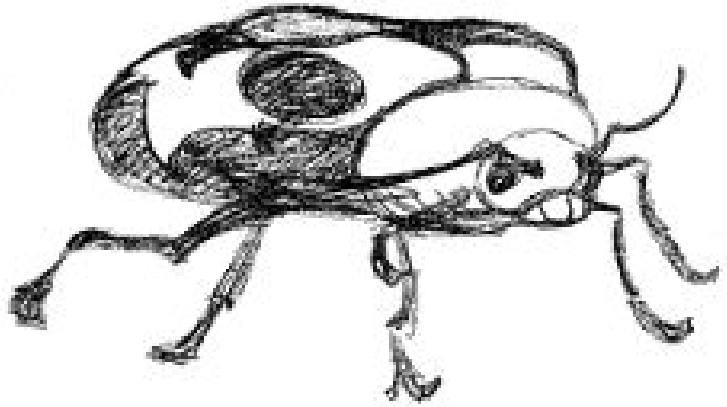
La prima trattazione rigorosa delle tipologie di attacco basate sulla statistica è attribuita ad Al Kindi un matematico autore di un libro pubblicato nel 801 DC in Arabia

Tecniche di Attacco

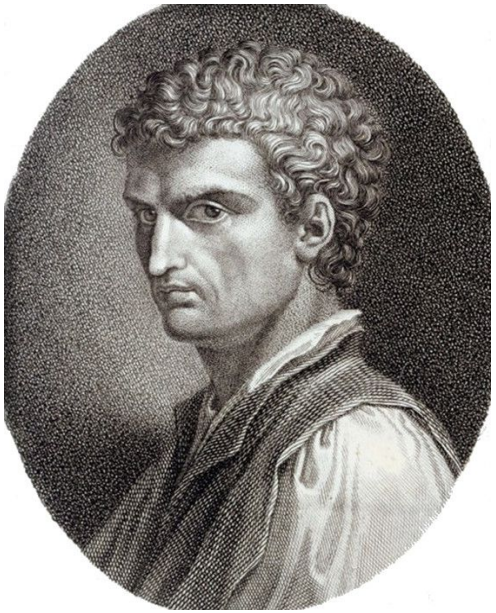
Gli attacchi statistici sono stati assimilati nella cultura popolare fino a diventare oggetto di opere letterarie:

- Artur Conan Doyle “L’avventura degli uomini danzanti” (1903)
- Edgar Allan Poe “Lo scarabeo d'oro” (1843)





Crittografia nella Storia - 4



- Leon Battista Alberti – 1467 DC

Cifratura Polialfabetica

Cifrari diversi per parti diverse di un messaggio

Formula o Cifrario a disco

Composto da 24 settori

- Esterno – Maiuscolo – Testo in chiaro
- Interno – Minuscolo – Testo cifrato

Crittografia nella Storia - 5

- Bellaso/Vigenerè – 1553/1585 DC

Cifratura Polialfabetica

Usa una parola chiave

Ogni lettera è “spostata” di un numero di caratteri pari al numero ordinale della lettera corrispondente della parola chiave.

```
Testo in chiaro: RAPPORTOIMMEDIATO
Chiave:          CHIAVECHIAVECHIAV
Testo cifrato:   UIYQKWWWRNIJGQJUK
```

Principi della Crittografia - 2

- Auguste Kerckoffs – 1883 DC

1)Il sistema deve essere praticamente, se non matematicamente, indecifrabile

2)Il sistema non deve essere segreto, dev'essere in grado di cadere nelle mani del nemico senza inconvenienti

3)La chiave deve essere comunicabile senza l'aiuto di note scritte e facilmente modificabile

Principi della Crittografia – 3

- Auguste Kerckoffs – 1883 DC

4)Il sistema deve essere applicabile alla corrispondenza telegrafica

5)Il sistema deve essere portatile e il suo utilizzo e uso non deve richiedere il concorso di più persone

6)È necessario che la sua applicazione sia facile da usare e che non richieda la conoscenza e l'uso di una lunga serie di regole

Principi della Crittografia - 4

Principio di Kerckoffs:

La sicurezza di un sistema crittografico non deve dipendere dal tener celato l'algoritmo crittografico. La sicurezza deve dipendere solo dal tener celata la chiave.

Massima di Shannon:

Il nemico conosce il sistema: Un sistema dovrebbe essere progettato sotto l'assunzione che il nemico guadagnerà immediatamente familiarità con esso.

Crittografia nella Storia - 6

- Seconda guerra mondiale – 1939 / 1945 DC

Macchina Enigma

Chiave Crittografica

La chiave in informatica è una **sequenza segreta di bit**

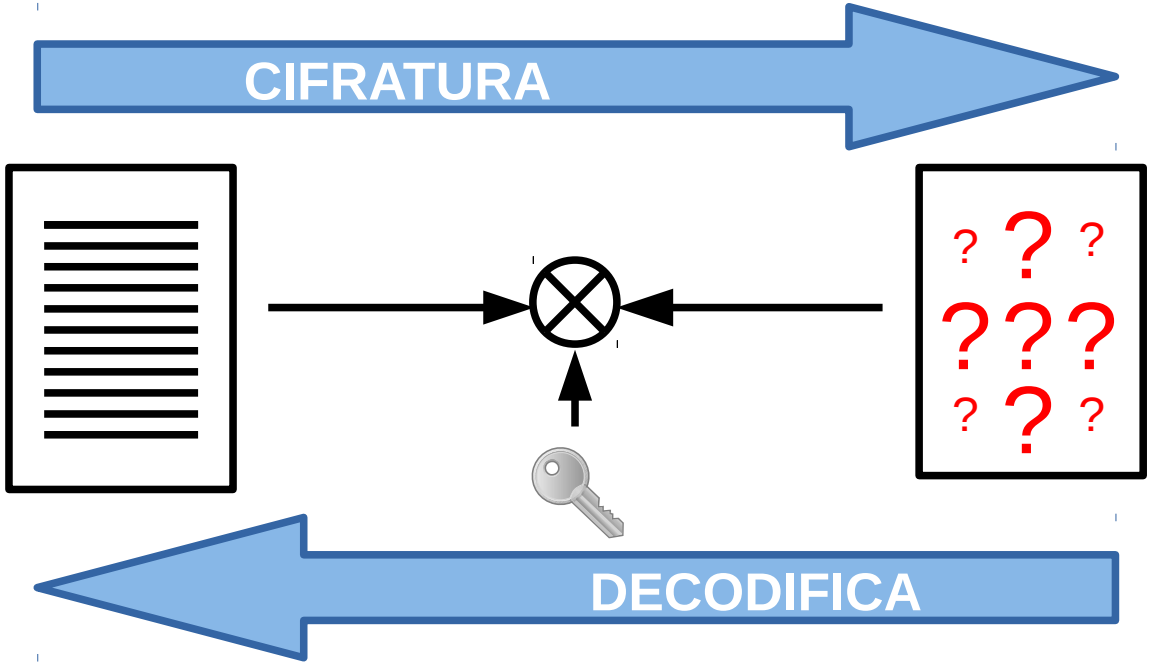
Caratteristiche della chiave:

- La chiave deve avere lunghezza finita configurabile
- La chiave deve essere generata in maniera casuale e necessità perciò di una sorgente casuale

Crittografia Simmetrica - 1

La chiave segreta deve essere condivisa solo tra mittente e destinatario

Es:
Macchina Enigma,
Zip



Problema: Il trasferimento della chiave richiede un canale sicuro

Crittografia Simmetrica - 2

Caratteristiche degli algoritmi simmetrici:

- Segretezza
- Autenticazione implicita del mittente
  Solo interlocutori hanno copia della chiave
- Integrità dell'informazione
  L'alterazione del messaggio comporta che la decodifica produca testo privo di senso
- Canale sicuro per il trasferimento della chiave
  L'intercettazione della chiave comporta il decadimento di tutti i vantaggi

Crittografia Asimmetrica - 1

Scopo: Risolvere il problema del canale sicuro per lo scambio delle chiavi

Principio: Usare proprietà matematiche note difficilmente reversibili (Equazioni asimmetriche o Funzioni unidirezionali)

Prima dimostrazione pratica del principio: Algoritmo Diffie – Hellman – Merkle 1976 DC

Crittografia Asimmetrica - 2

Utilizza coppia di chiavi:

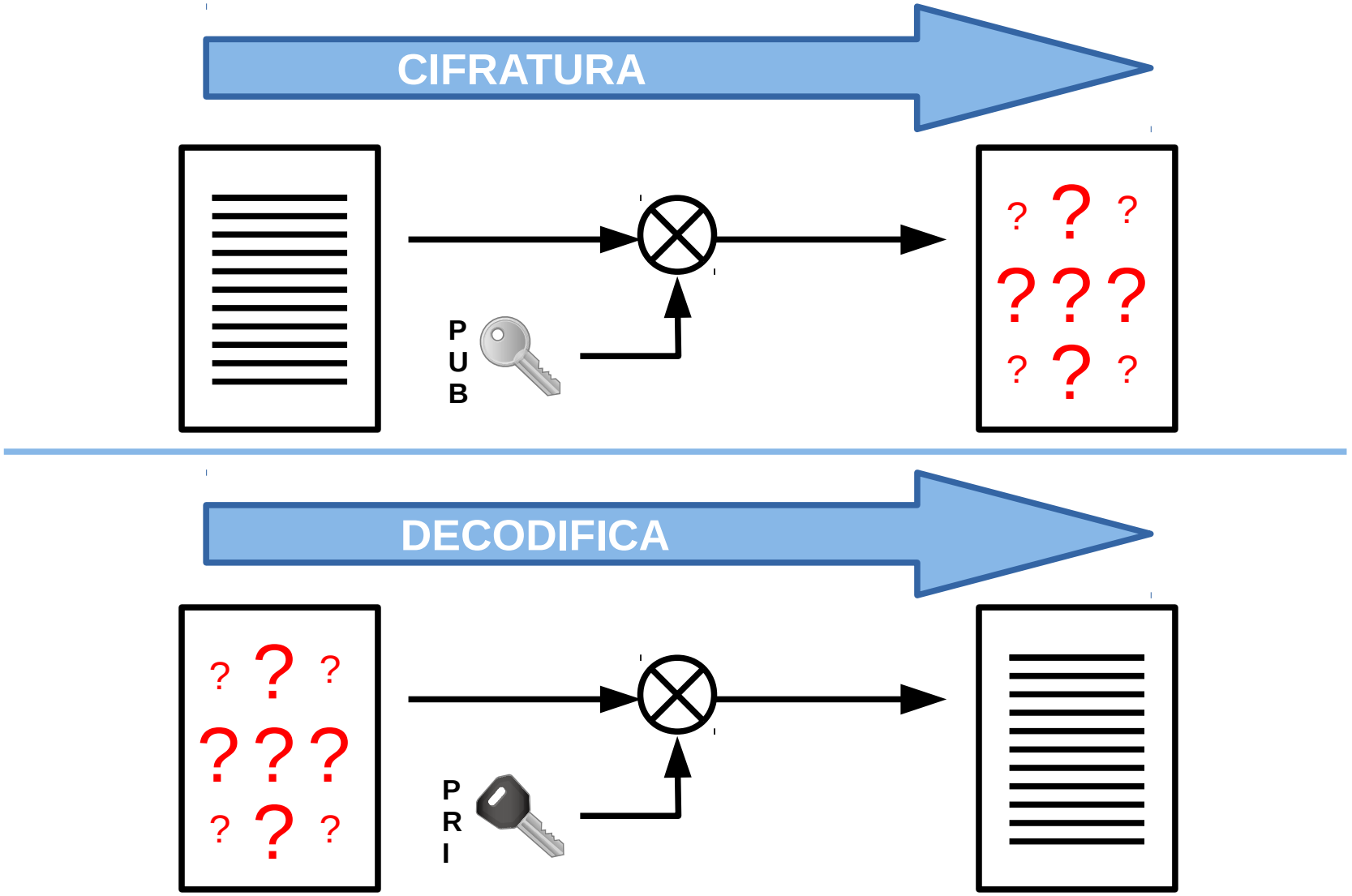
- Pubblica - Usata per cifrare e firmare
- Privata - Usata per decifrare e firmare

Es: Algoritmo DSA, Algoritmo RSA

Per comunicare sono necessarie:

- Propria coppia di chiavi
- La chiave pubblica di ognuno dei destinatari

Crittografia Asimmetrica – 3



Crittografia Asimmetrica - 4

Caratteristiche degli algoritmi asimmetrici:

- La lunghezza della chiave deve essere maggiore rispetto agli algoritmi simmetrici

- Una chiave pubblica è meno sicura di una chiave segreta
  - 2048 bit pubblica ≈ 128 bit segreta
  - 4096 bit pubblica ≈ 144 bit segreta

- L'autenticazione deve essere esplicita perché la chiave pubblica è disponibile a tutti

Crittografia Asimmetrica - 5

L'autenticazione è eseguita mediante doppia cifratura:

- Il mittente firma il documento usando la propria chiave privata
- Il mittente cifra il documento usando la chiave pubblica del destinatario
- Il destinatario decifra il documento usando la propria chiave privata
- Il destinatario verifica la firma del mittente utilizzando la sua chiave pubblica

Chiave Asimmetrica - 1

Si basa sulle proprietà dei numeri primi:
Numeri ℕ divisibili solo per loro stessi o per 1

Dati due numeri primi ricavarne il prodotto

$$N1 * N2 = M$$

È un'operazione banale

Dato il prodotto, la fattorizzazione

$$M = N1 * N2$$

È un'operazione complessa se entrambi i numeri sono ignoti a priori

Chiave Asimmetrica - 2

Chiave pubblica: Si utilizza il prodotto M

Chiave privata: Si utilizza uno dei moltiplicandi

Cifre del numero primo α Lunghezza chiave
- Sicurezza α Lunghezza chiave
- Prestazioni α 1 / Lunghezza chiave

Crittografia Ellittica

Si basa su due “problemi” matematici:

- Le curve ellittiche
- I campi finiti

L'operazione $a^x = b$ è banale, ma l'inversa $x = \log a(b)$ è complicata nel campo finito

Una curva ellittica è un'equazione $y^2 = x^3 + ax + b$
La cui soluzione rende un campo finito

“Logaritmi discreti in sottogruppi ciclici di curve ellittiche su campi finiti”

Crittografia Quantistica

Gilbert Vernam nel 1918 propose di utilizzare un cifrario di Bellaso / Vigenerè con una lunghezza di chiave pari a quella del messaggio

La robustezza dell'algoritmo fu dimostrata matematicamente da Claude Shannon nel 1949

- Unico algoritmo la cui inviolabilità è dimostrata

É fondamentale che la chiave sia univoca poiché il riutilizzo indebolisce contro la crittoanalisi

Le proprietà della fisica quantistica garantiscono l'univocità della chiave alla creazione

OpenPGP

Standard aperto per la crittografia

- Introdotto nel 1991 con il programma PGP
- Largamente adottato
- Robustezza giudicata immediatamente inferiore a quella militare
- Utilizza sia la crittografia simmetrica che quella asimmetrica
- Progettato per il traffico e-mail ed in seguito ampliato per cifrare file, dischi e linee di comunicazione (VPN)

GNU Privacy Guard (GPG)

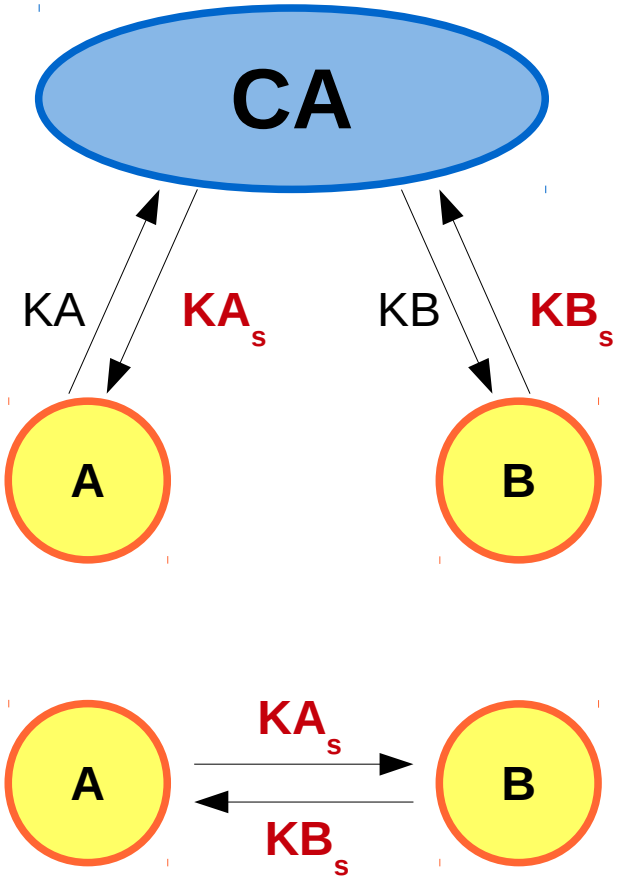
- Programma Open Source gratuito
- Gestisce sia e-mail che file
- Multi-piattaforma (Android, Linux, Mac, Win)

Funzionalità principali:

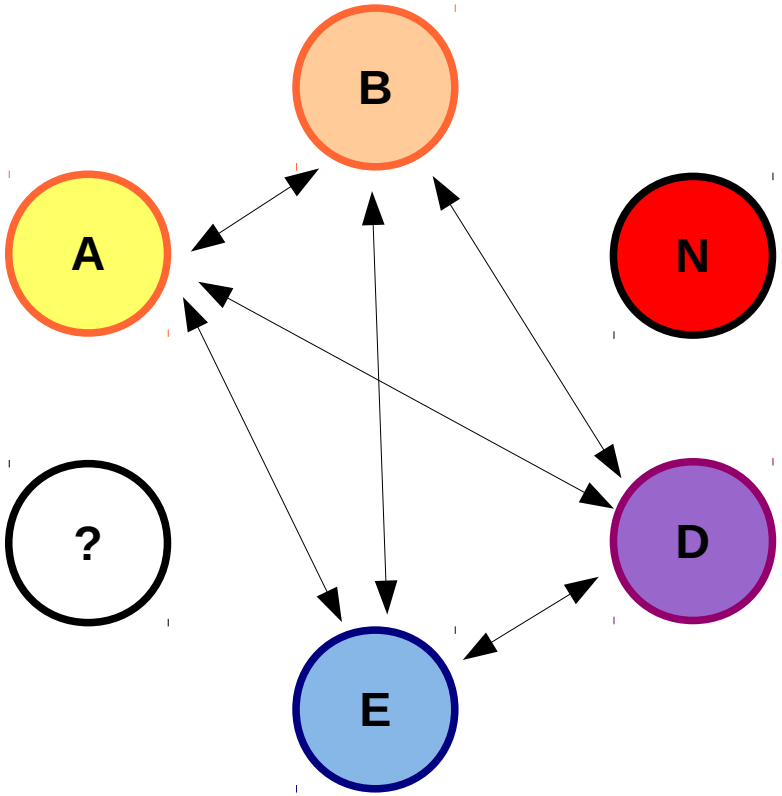
- Codifica, decodifica, firma e verifica dell'integrità delle informazioni
- Creazione e gestione delle chiavi
- Gestione della fiducia sia gerarchica (Certification Authority) che distribuita (Web Certification)

Fiducia (Trust)

HIERARCHY



WEB OF TRUST



Web of Trust

Ogni utente possiede due portachiavi (Keyring):

- Privato: Contiene solo le chiavi dell'utente
- Pubblico: Contiene le chiavi pubbliche importate da altri utenti

Si assegna un livello ad ogni chiave:

- Unknown
- Never: Firme mai valide
- Marginal: Servono un minimo di 3 firme
- Full: Firma sempre valida
- Ultimate: Solo le chiavi personali

EncFS - Introduzione

Strumento per cifrare file system in maniera trasparente

Crea un file system virtuale in cui salva i dati cifrati ed una cartella attraverso cui accedere ai file in chiaro

~/crypt/.encrypt è la cartella con i dati cifrati
~/crypt/encrypt è la cartella attraverso cui manipolare i dati

EncFS - Portabilità

I software che lavorano per blocchi solitamente sono limitati ad un singolo sistema operativo:

- BitLocker (Windows) / Truecrypt (Windows XP)
- eCryptFS (Linux)
- FileVault (MacOsX)
- Geli (FreeBSD) / Softraid (OpenBSD)

EncFS è portabile:

- Disponibile per qualsiasi Linux / Unix
- Disponibile per MacOsX e Windows attraverso Boxcryptor o Safe

EncFS - Vantaggi

- Può appoggiarsi su file system locali, remoti, Spazio cloud o dischi rimovibili
- Non usa interi volumi
- Buone prestazioni
- Semplice eseguire back-up o copie dei dati
- Semplice trasferire i dati cifrati su supporti rimovibili
- Eventuali corruzioni di dati sono limitate a singoli file

EncFS - Svantaggi

- Non usa la crittografia per i metadati, ma solo per i nomi dei file ed il loro contenuto
- Un attaccante può ricavare facilmente numero e dimensioni dei file (Con uno scarto di 8 / 16 byte)
- Utilizza la medesima chiave per tutti i file
- La chiave è passibile di attacchi da chiunque abbia accesso a più versioni del cifrario

Collegamenti

GNU Privacy Guard

- https://www.gnupg.org
- https://www.gpg4win.org
- https://gpgtools.org/gpgsuite.html

EncFS

- https://github.com/vgough/encfs
- http://www.getsafe.org/about
- https://www.boxcryptor.com/en

Informazioni & Licenze