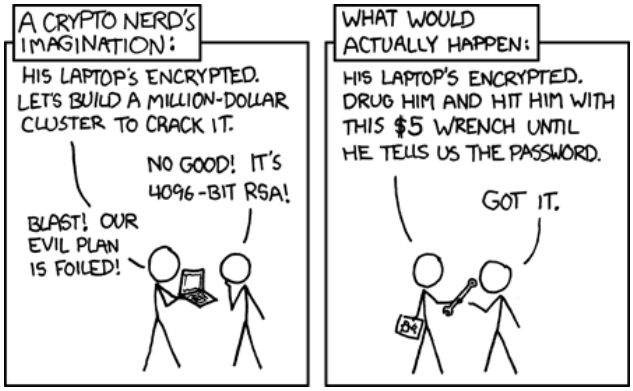
crittoanalisi



crittoanalisi = lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è richiesta per cifrare.
La CA di norma esclude altri metodi di attacco come ad esempio la corruzione, la coercizione fisica, il furto, l'ingegneria sociale (metodi spesso più produttivi della CA tradizionale).

crittoanalisi: principio di Kerckhoffs

L'attaccante, Eve, può conoscere il crittosistema usato da Alice e Bob.
Non conosce la chiave.
Vantaggi:

- è più facile tenere segreta la chiave
- se la sicurezza si basa sulla chiave, e la chiave viene scoperta, basta cambiare chiave
- si può usare lo stesso crittosistema per far comunicare diverse coppie di persone

- oggi il principio di Kerckhoffs viene inteso in maniera più forte: l'algoritmo deve essere pubblico
- un sistema che viene molto studiato (e attaccato) è più sicuro
- meglio che le debolezze, se ci sono, vengano scoperte e rese pubbliche
- se l'algoritmo è pubblico, non c'è rischio di reverse engineering
- si possono stabilire standard

crittoanalisi: tipi di attacco

Ciphertext only attack: L'attaccante conosce una stringa y di testo cifrato. Cerca di risalire al testo in chiaro o alla chiave.

Known plaintext attack: L'attaccante conosce una stringa x di testo in chiaro e il corrispondente testo cifrato y. Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen plaintext attack: L'attaccante ha la possibilità di scegliere un testo in chiaro x e di ottenere il corrispondente testo cifrato. Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen ciphertext attack: L'attaccante ha la possibilità di scegliere un testo cifrato y e di ottenere il corrispondente testo in chiaro x. Cerca di risalire alla chiave.

crittoanalisi di un cifrario a sostituzione

Dobbiamo decrittare il testo

```
QANGH TGMYJ XGHTN AVUNG TTYSH LUXYU OUAUD UQQYJ UJAXX
YNUTY NGKGB BUGMA XASLG KJUGX YQANG HTGMY JXGHT DABBY
VUJAK TYTYT ANGHT JAKTY VUJHS SYOGH TSAOD JUQAD ABBYV
GQGXG SXGVU IHAJJ UQPAV UTMAN TYSUO AXXYT YTAJJ ASXHF
AATAU QGOUT AXXUD ANGQQ ATVAN AUJFH YQYAD ANNUS QGJVG
NAJAS XGTBA TYTSY QYOAG TVGSS AOGUJ FGXXY KJUAQ PAHTL
AJKUY NTYIH ASXYD ABBYV UJAKT YQGDU XYTAJ JGLYX XAKGV
UHTMA QQPUY FGJAK TGOAU JIHGJ AGMAM GTYOA OGSXN GTXYT
UYSAT YTQPA XHXXU JYQPU GOGMG TYOGA SXNYQ UJUAK UGDAN
MUGVA JJGDH TXGVA JSHYT GSYQP AANGS AODNA JHSXN GADGY
TGBBG QYOAH TGQUJ UAKUG OGXHN GGDDA TGOGA SXNYQ UJUAK
UGALL AMUSX YIHAJ DABBY VUJAK TYSUN GJJAK NYXHX XYAVG
```

analisi delle frequenze

frequenze dei caratteri % in italiano

A	B	C	D	E	F	G	H	I
10,41	0,95	4,28	3,82	12,62	0,75	2,01	1,10	11,62
J	K	L	M	N	O	P	Q	R
0	0	6,61	2,58	6,49	8,71	3,20	0,75	6,70
S	T	U	V	W	X	Y	Z	
6,04	6,06	3,04	1,51	0	0	0	0,93	

analisi delle frequenze

frequenze dei caratteri % nel nostro testo

A	B	C	D	E	F	G	H	I
13,52	2,41	0	2,78	0	0,74	11,30	4,26	0,74
J	K	L	M	N	O	P	Q	R
6,85	2,59	1,11	1,85	4,44	2,96	1,11	4,44	0
S	T	U	V	W	X	Y	Z	
4,44	7,78	8,52	2,78	0	6,48	8,89	0	

proviamo A=e

```
QeNGH TGMYJ XGHTN eVUNG TTYSH LUXYU OUeUD UQQYJ UJeXX
YNUTY NGKGB BUGMe XeSLG KJUGX YQeNG HTGMY JXGHT DeBBY
VUJeK TYTYT eNGHT JeKTY VUJHS SYOGH TSeOD JUQeD eBBYV
GQGXG SXGVU IHeJJ UQPeV UTMeN TYSUO eXXYT YTeJJ eSXHF
eeTeU QGOUT eXXUD eNGQQ eTVeN eUJFH YQYeD eNNUS QGJVG
NeJeS XGTBe TYTSY QYOeG TVGSS eOGUJ FGXXY KJUeQ PeHTL
eJKUY NTYIH eSXYD eBBYV UJeKT YQGDU XYTeJ JGLYX XeKGV
UHTMe QQPUY FGJeK TGOeU JIHGJ eGMeM GTYOe OGSXN GTXYT
UYSeT YTQPe XHXXU JYQPU GOGMG TYOGe SXNYQ UJUeK UGDeN
MUGVe JJGDH TXGVe JSHYT GSYQP eeNGS eODNe JHSXN GeDGY
TGBBG QYOeH TGQUJ UeKUG OGXHN GGDDe TGOGe SXNYQ UJUeK
UGeLL eMUSX YIHeJ DeBBY VUJeK TYSUN GJJeK NYXHX XYeVG
```

Digrammi frequenti in italiano (nell'ordine):

er, es, on, re, el, en, de, di, si, ti, la, al
Nel nostro testo:

AN (9), YT (9), AJ (6), VU (5).
(le nostre vocali sono probabilmente G, U, Y)
G=a, N=r, ?? Y=o, T=n, U=i ??.

```
QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa
```

```
QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa
```

X=t

```
QeraH naMoJ taHnr eVira nnoSH Litoi OieiD iQQoJ iJett
orino raKaB BiaMe teSLa KJiat oQera HnaMo JtaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQata StaVi IHeJJ iQPeV inMer noSim etton oneJJ eStHF
eenei QaOin ettiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS tanBe nonSo QoOea nVaSS eOaiJ Fatto KJieQ PeHnL
eJKio rnoIH eStoD eBBoV iJeKn oQaDi toneJ JaLot teKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe maStr anton
ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer
MiaVe JJaDH ntaVe JSHon aSoQP eeraS eODre JHStr aeDao
naBBa QoOeH naQiJ ieKia OatHr aaDDe naOae StroQ iJieK
iaeLL eMiSt oIHeJ DeBBo ViJeK noSir aJJeK rotHt toeVa
```

```
                                  aMeM anoOe OaStr anton
ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer
```

M=v, S=s, O=m.....

la sostituzione è

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
G L Q V A F K P U - - J O T Y D I N S X H M - - - B
```

il testo in chiaro è:

```
cerau navol taunr edira nnosu bitoi mieip iccol ilett
orino ragaz ziave tesba gliat ocera unavo ltaun pezzo
dileg nonon eraun legno dilus somau nsemp licep ezzod
acata stadi quell iched inver nosim etton onell estuf
eenei camin ettip eracc ender eilfu ocoep erris calda
reles tanze nonso comea ndass email fatto gliec heunb
elgio rnoqu estop ezzod ilegn ocapi tonel labot tegad
iunve cchio faleg namei lqual eavev anome mastr anton
iosen onche tutti lochi amava nomae stroc ilieg iaper
viade llapu ntade lsuon asoch eeras empre lustr aepao
nazza comeu nacil iegia matur aappe namae stroc ilieg
iaebb evist oquel pezzo dileg nosir alleg rotut toeda
```

crittografia a chiave pubblica

Whitfield Diffie

Martin Hellman

New Directions in Cryptography

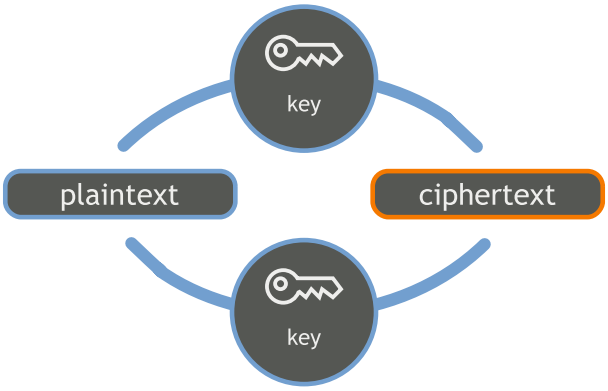
We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware . . . has brought the cost of high grade cryptographic devices down to where it can be used in . . . remote cash dispensers and computer terminals. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

Diffie e Helmann, IEEE IT **22** (1976)

- nel 1976, Diffie e Hellman pubblicano “New directions in cryptography”
- viene considerato l’inizio della crittografia a chiave pubblica (PKC)
- propongono uno schema di scambio della chiave basato sul logaritmo discreto
- introducono l’idea di un crittosistema a chiave pubblica
- la prima realizzazione di un crittosistema di questo tipo si ha nel 1978 con l’RSA

crittografia simmetrica

- Alice e Bob condividono la stessa chiave k – scelta e scambiata fra loro prima di cominciare a comunicare
- la chiave dà luogo a una funzione di cifratura e_k e una funzione di decifratura d_k
- è facile ricavare d_k da e_k
- se si sa cifrare, si sa anche decifrare

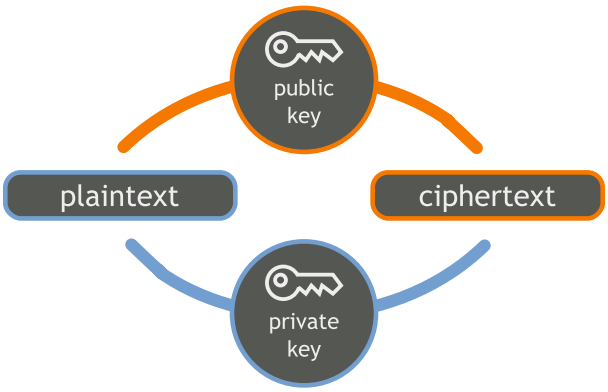


come condividere la chiave?

- prima di cominciare a comunicare Alice e Bob devono scegliere una chiave segreta
- usando un canale sicuro
- se l'avversario intercetta la chiave, la comunicazione è completamente compromessa

idea della crittografia a chiave pubblica

- sviluppare un crittosistema in cui data la funzione di cifratura e_k sia computazionalmente difficile determinare d_k
- Bob rende pubblica la sua funzione di cifratura e_k
- Alice (e chiunque altro) può scrivere a Bob, cifrando il messaggio con la e_k senza bisogno di accordi preliminari
- Bob è l'unico che può decifrare il messaggio
- analogia con un lucchetto, che chiunque può usare, ma di cui solo Bob ha la chiave



funzioni unidirezionali

- bisogna che la funzione di cifratura e sia una funzione unidirezionale (one-way function)
- informalmente, una funzione invertibile $f : \mathcal{P} \to \mathcal{C}$ si dice unidirezionale se
  - dato $x \in \mathcal{P}$, il calcolo di $f(x)$ è facile
  - per quasi tutti gli $y \in \mathcal{C}$ il calcolo di $f^{-1}(y)$ è difficile
  - dato $x \in \mathcal{P}$, il calcolo di $f(x)$ è realizzabile con una complessità polinomiale
  - per quasi tutti gli $y \in \mathcal{C}$ il calcolo di $f^{-1}(y)$ non è realizzabile con una complessità polinomiale
- Esempio una funzione ritenuta unidirezionale: sia $n = pq$, p e q numeri primi "abbastanza grandi", b un intero coprimo con $\phi(n)$; sia $f : \mathbb{Z}_n \to \mathbb{Z}_n$ t.c.

$$f(x) = x^b \pmod{n}$$

trapdoor

- se la funzione è unidirezionale, anche per Bob è impossibile decifrare il messaggio
- una trapdoor (botola) one-way function è una funzione unidirezionale che diventa facile da invertire, se si conosce un'informazione supplementare
- l'informazione supplementare viene tenuta segreta da Bob, e usata per decifrare
  - ci sarà una chiave pubblica nota a tutti – che serve per cifrare
  - e una chiave privata nota solo a Bob – che serve per decifrare

cenni sulla complessità computazionale

- come si misura la complessità computazionale di un algoritmo?
- si parla di algoritmi che operano su numeri interi
  - ex: dati due interi trovare la somma, il prodotto, il MCD
- il "tempo" di esecuzione dipende dalla grandezza dell'input
- la grandezza di un input N è pari al numero di bit nella sua rappresentazione binaria ($\approx \log_2 N$)
- la complessità di un algoritmo si misura in termini di operazioni bit
- sono operazioni bit:
  - addizione fra due cifre binarie (es. $0 + 1$);
  - sottrazione fra due cifre binarie (es. $1 - 0$);
  - moltiplicazione fra due cifre binarie (es. $1 \cdot 1$);
  - divisione di un intero a *due* cifre binarie per *una* cifra binaria (es. 10 diviso 1);
  - traslazione a *sinistra* di un posto, cioè moltiplicazione per 2, e traslazione a *destra* di un posto, cioè divisione per 2.

complessità polinomiale e esponenziale

Definizione

La complessità computazionale di un algoritmo che opera sugli interi è data dal numero di operazioni bit occorrenti per eseguirlo.

è una funzione (della lunghezza dell'input)

Definizione

Un algoritmo $\mathcal{A}$ per eseguire un calcolo su numeri interi si dice polinomiale se esiste un intero positivo d tale che il numero di operazioni bit necessarie per eseguire l'algoritmo su interi di lunghezza binaria al più k è $\mathcal{O}(k^d)$.

Definizione

Un algoritmo si dice esponenziale se il numero di operazioni bit necessarie per eseguire l'algoritmo su interi di lunghezza binaria al più k è dello stesso ordine di 2^{ck}, per una costante $c > 0$

- polinomiale $\leftrightarrow$ (computazionalmente) facile
- esponenziale $\leftrightarrow$ (computazionalmente) difficile
- mostare che esiste un algoritmo polinomiale che risolve un dato problema è semplice - basta descrivere l'algortimo
- ma come si fa a mostare che non esiste un algoritmo polinomiale che risolve un dato problema?