

# Crittografia

Federico Matteoni

A.A. 2020/21



# Indice

<b>1</b>	<b>Introduzione alla Crittografia</b>	<b>7</b>
1.1	Introduzione . . . . .	7
1.1.1	Lo scenario . . . . .	7
1.1.2	Antichi esempi . . . . .	8
1.2	Livello di segretezza . . . . .	8
1.2.1	Chiavi segreta . . . . .	8
1.2.2	Crittoanalista . . . . .	9
1.2.3	Situazione attuale . . . . .	9
1.2.4	Cifrari odierni . . . . .	9
1.3	Rappresentazione matematica di oggetti . . . . .	10
1.4	Richiamo della teoria della calcolabilità . . . . .	11
1.4.1	Algoritmi . . . . .	12
1.4.2	Modelli di calcolo . . . . .	12
1.4.3	Decidibilità e trattabilità . . . . .	13
1.4.4	Tipologie di problemi . . . . .	13
1.4.5	Classi di complessità . . . . .	14
1.4.6	Certificato . . . . .	14
1.4.7	Classi co-P e co-NP . . . . .	15
<b>2</b>	<b>Sequenze Casuali</b>	<b>17</b>
2.1	Esempi di algoritmi numerici . . . . .	17
2.2	Casualità . . . . .	18
2.2.1	Sequenze casuali . . . . .	18
2.2.2	Sorgente binaria casuale . . . . .	19
2.3	Test statistici . . . . .	20
2.4	Generatori crittograficamente sicuri . . . . .	20
2.4.1	Generatori di numeri pseudocasuali basati su cifrari simmetrici . . . . .	21
2.5	Algoritmi randomizzati . . . . .	21
2.5.1	Test di primalità (Miller, Rabin) . . . . .	22
2.5.2	Generazione di numeri primi . . . . .	23
2.6	Classe RP . . . . .	23
<b>3</b>	<b>Cifrari storici</b>	<b>25</b>
3.1	Principi di Bacone . . . . .	25
3.2	Antichi esempi . . . . .	25
3.2.1	Scitale . . . . .	25
3.2.2	Erodoto, Storie . . . . .	25
3.2.3	Enea Tattico . . . . .	25
3.2.4	Cifrario di Cesare . . . . .	26
3.3	Classificazione dei cifrari storici . . . . .	26
3.3.1	Cifrari a sostituzione . . . . .	26
3.3.2	Cifrari a trasposizione . . . . .	28
3.4	Crittoanalisi Statistica . . . . .	28

<b>4</b>	<b>Cifrari perfetti</b>	<b>31</b>
4.0.1	Teorema di Shannon . . . . .	31
4.0.2	One-Time Pad . . . . .	32
4.1	Principi di Shannon . . . . .	33
4.2	Data Encryption Standard . . . . .	33
4.2.1	Varianti del DES . . . . .	36
<b>5</b>	<b>Crittografia a Chiave Pubblica</b>	<b>39</b>
5.1	AES . . . . .	39
5.1.1	Protocollo DH . . . . .	39
5.1.2	Cifrari simmetrici . . . . .	39
5.1.3	Cifrari asimmetrici . . . . .	39
5.2	RSA . . . . .	40
5.2.1	Generatori . . . . .	41
5.2.2	Crittografia a chiave pubblica . . . . .	43
5.2.3	Cifrari ibridi . . . . .	43
5.2.4	RSA . . . . .	43
5.3	Protocollo Diffie-Hellmann . . . . .	45
5.4	Cifrario di Elgamal . . . . .	46
<b>6</b>	<b>Elliptic Curve Cryptography</b>	<b>49</b>
<b>7</b>	<b>Esercizi</b>	<b>51</b>
7.1	Complessità e randomizzazione . . . . .	51
7.2	Cifrari Storici . . . . .	52
7.3	Cifrari Perfetti . . . . .	54
7.4	Cifrari Simmetrici . . . . .	55

## Introduzione

Prof.ssa: Anna Bernasconi.

Vedremo i cifrari da un punto di vista prettamente algoritmico. Vedremo anche i cifrari storici, ormai non più utilizzabili, perché hanno "aperto la strada", per poi passare ai cifrari perfetti (soluzione ideale ma con costo elevato).

Poi esamineremo i cifrari simmetrici, a chiave pubblica, curve ellittiche, firma digitale, SSL. Protocolli zero knowledge, blockchain e crittografia quantistica.

Libro di testo: Bernasconi, Ferragina, Luccio - Elementi di Crittografia.

**Esame** Orali nel caso di esami a distanza, scritto nel caso di esami in presenza, closed-book.



# Capitolo 1

## Introduzione alla Crittografia

### 1.1 Introduzione

**Crittografia** Significa "scrittura nascosta", si intendono tecniche matematiche per mascherare i messaggi per non renderli leggibili a terzi (**crittografia**) o tentare di svelarli quando non si è il legittimo destinatario (**crittoanalisi**). Quindi tecniche di protezione e viceversa.

Esiste per i due mondi in contrapposizione: persone che vogliono scambiarsi privatamente informazioni e gli *impiccioni* che desiderano ascoltare o intromettersi nelle conversazioni altrui (per curiosità, investigazione o altri scopi).

**Due gruppi di persone** Chi vuole proteggersi userà **metodi di cifratura**, gli altri useranno **metodi di crittoanalisi**

**Crittografia** Metodi di Cifratura

**Crittoanalisi** Metodi di ... **crittologia** studio comunicazione canali non sicuri e relativi problemi

#### 1.1.1 Lo scenario

Alice vuole comunicare con Bob su un canale insicuro, quindi adottano un metodo di cifratura per spedire il messaggio in chiaro  $m$  sottoforma di crittogramma  $c$  (testo cifrato) che deve essere: incomprensibile al crittoanalista Eve (eavesdropper) in ascolto sul canale, ma facilmente decifrabile da Bob.

**MSG** Insieme dei messaggi in chiaro

**CRITTO** Insieme dei crittogrammi

$C : \text{MSG} \rightarrow \text{CRITTO}$

$D : \text{CRITTO} \rightarrow \text{MSG}$

Sono operazioni da poter fare in tempo polinomiale.  $C$  e  $D$  sono una l'inversa dell'altra, ma  $C$  **deve essere iniettiva**.



### 1.1.2 Antichi esempi

**Erodoto** Nelle *Storie*, V secolo a.C.

Messaggi tatuati sulla testa, coperti dai capelli e riscoperti rasando la testa.

**Scitale** Spartani. Asta cilindrica in due esemplari identici. Si avvolgeva una striscia di carta attorno al cilindro e scritta. La chiave del cifrario è il diametro dello scitale.



**Enea Tattico** Un libro qualsiasi con un insieme di lettere segnate, o sostituire le vocali con simboli grafici.

**Cifrario di Cesare** Il più antico cifrario di concezione moderna. L'idea di base è che il crittogramma è ottenuto dal messaggio in chiaro  $m$  sostituendo ogni lettera con quella di tre posizioni più avanti nell'alfabeto.

Es.  $A \rightarrow D$ ,  $Z \rightarrow C$ . La segretezza dipende interamente dalla conoscenza del metodo, era destinato all'uso ristretto da un piccolo gruppo di persone.

## 1.2 Livello di segretezza

**Classificazione** in base al livello di segretezza

Cifrari per **uso ristretto**

Le tecniche con cui si calcola e decifra il crittogramma sono tenute segrete in ogni loro aspetto. Impiegati per comunicazioni classificate (diplomatiche o militari), non adatti per uso di massa.

Cifrari per **uso generale**

Ogni codice segreto non può essere mantenuto tale per troppo a lungo. La parte segreta si limita alla chiave, nota solamente agli utenti che stanno comunicando.

Vengono studiati dalla comunità, coinvolgendo tantissime persone. Solo la chiave deve essere segreta.

**Il nemico conosce il sistema.**

Quindi  $C$  e  $D$  sono note, la chiave **segreta**  $k$  è usata come input sia in  $C$  che in  $D$ :

$$c = C(m, k), m = D(c, k)$$

Se non si conosce  $k$ , anche conoscendo  $C$  e  $D$  non si possono estrarre informazioni dal crittogramma.

Tenere segreta una sola chiave è più facile che segretare l'intero metodo. Tutti possono usare  $C$  e  $D$  pubbliche con chiavi diverse, e se un crittoanalista entra in possesso di una chiave posso generarne semplicemente una nuova.

### 1.2.1 Chiavi segreta

Se la segretezza dipende unicamente dalla chiave bisogna proteggersi dagli attacchi a forza bruta, quindi avere un gran numero di chiavi, così da essere immuni da chi le prova tutte.

Inoltre la chiave deve essere scelta in modo casuale e non prevedibile, sennò il crittoanalista può provare le chiavi ovvie.

**Attacco esauriente** Il crittoanalista potrebbe sferrare un attacco a forza bruta verificando la significatività delle sequenze  $D(c, k) \forall k$ .

Se  $|Key| = 10^{20}$  e con un calcolatore che impiega  $10^{-6}$  per calcolare  $D(c, k)$  servirebbe in media più di un milione di anni per scoprire il messaggio provando tutte le chiavi. Però la segretezza può essere violata con altre tecniche: esistono cifrari più sicuri di altri pur con uno spazio di chiavi più piccoli.

Un cifrario complicato non è necessariamente più sicuro e **mai sottovalutare la bravura del crittoanalista**.



## 1.2.2 Crittoanalista

**Comportamento** Il comportamento di un crittoanalista può essere:

**Passivo**, quando si **limita ad ascoltare** la comunicazione

**Attivo**, quando **agisce sul canale** disturbando la comunicazione o modificando il contenuto dei messaggi.

**Attacchi a un sistema crittografico** Hanno l'obiettivo di forzare un sistema. Il metodo e il livello di pericolosità dipendono dalle informazioni in possesso del crittoanalista:

**Cipher Text Attack**: conosce una serie di crittogrammi

**Known Plain-Text Attack**: conosce una serie di coppie ( $m$ ,  $c$ )

**Chosen Plain-Text Attack**: si procura coppie ( $m$ ,  $c$ ) relative a messaggi in chiaro da lui scelti.

Tutta la crittografia a chiave pubblica è soggetta a questo tipo di attacco (avendo la chiave pubblica, cifro dei messaggi che penso possano passare e ascolto finché non trovo nella comunicazione i crittogrammi in mio possesso).

**Man in the Middle** Il crittoanalista si installa sul canale di comunicazione:

**Interrompe le comunicazioni dirette** tra gli utenti Alice e Bob

le **sostituisce con messaggi propri**

e **convince** ciascun utente **che tali messaggi provengano legittimamente dall'altro** utente.

Quindi il crittoanalista **Eve si finge Bob agli occhi di Alice e Alice agli occhi di Bob**.

**Esiti**

Successo pieno, si scopre completamente  $D$  o si ottiene la chiave

Successo limitato, si scopre solo qualche informazione ma sufficiente per comprendere il messaggio

## 1.2.3 Situazione attuale

**Cifrari perfetti** Inattaccabili, esistono ma richiedono operazioni complesse, **chiavi lunghe tanto quanto il messaggio e mai riutilizzabili**.

**Shannon**, 1945 (pubblicato nel 1949 per motivi di segretezza militare):  $m$  e  $c$  appaiono totalmente scorrelati, come se  $c$  fosse una stringa casuale di bit.

Nessuna informazione può filtrare dal crittogramma. Vedremo la teoria matematica.

**One-Time Pad** Anche detto blocco monouso, sicuro ma per essere usato bene richiede chiavi segrete totalmente casuali e lunghe quanto il messaggio. Come generarla e come scambiarla?

**Cifrari attuali** Nella crittografia di massa non si usano cifrari perfetti, ma **cifrari dichiarati sicuri**, inviolati dagli esperti e che usano algoritmi solo esponenziali per decrittare senza chiave. Il tempo per violare un cifrario è enorme e rende l'operazione insostenibile  $\rightarrow$  impossibilità *pratica* di forzare il cifrario.

**Dichiarati sicuri** Non è noto se questi problemi matematici richiedano algoritmi *necessariamente* esponenziali o se sono dovuti all'incapacità nostra di trovare metodi più efficienti. Si riconduce a  $P = NP$

## 1.2.4 Cifrari odierni

**Advanced Encryption Standard** AES, simmetrico a blocchi con chiavi di 128-256bit, pubblicamente noto e realizzabile su computer di ogni tipo. Il messaggio è diviso a blocchi lunghi quanto la chiave.

**Le chiavi** Sono stabilite dai mezzi elettronici (PC, smartphone, terminale...) e su Internet si scambia una chiave per ogni sessione.

**Scambio delle chiavi** La chiave va comunicata in sicurezza su un canale non ancora sicuro. Un'intercettazione nello scambio della chiave compromette il sistema.

Nel 1976 viene proposto un algoritmo per generare e scambiare una chiave segreta su un canale insicuro, senza necessità di scambiare informazioni o di incontrarsi in precedenza.

Si chiama **protocollo DH**, ancora largamente utilizzato nei protocolli crittografici su Internet.

Si scambiano pezzi di chiave tramite la rete e unendole a informazioni locali si costruisce la chiave.

**Chiave pubblica** Diffie ed Hellman hanno anche proposto la crittografia a chiave pubblica.

**Cifrari simmetrici:** stessa chiave per cifrare e decifrare, nota solo ai due utenti che comunicano. La scelgono di comune accordo e la tengono segreta.

**Cifrari asimmetrici:** chiavi pubbliche usate per cifrare e chiavi private per decifrare.

$c = C(m, k_{pub})$

$m = D(c, k_{priv})$

Si rende necessario che la  $C$  sia una one-way trapdoor: calcolare il crittogramma deve essere facile (polinomiale), ma decifrare  $c$  deve essere computazionalmente difficile (a meno di conoscere la trapdoor, la chiave privata).

**RSA** Rivest, Shamir, Adleman, 1977. Propongono un sistema a chiave pubblico facile da calcolare e difficile da invertire.

### Vantaggi

Comunicazione molti a uno

Tutti possono inviare in modo sicuro allo stesso destinatario usando la sua chiave pubblica, ma solo lui può decifrarli. Un crittoanalista non può decifrare anche se conosce  $C$ ,  $D$  e  $k_{pub}$

Se  $n$  utenti vogliono comunicare servono solo  $2n$  chiavi invece delle  $n(n-1)/2$  necessarie nei cifrari simmetrici (una coppia per ogni coppia di utenti)

Non è richiesto nessun scambio

### Svantaggi

Sono molto lenti rispetto ai cifrari simmetrici (polinomi di terzo grado)

Sono esposti ad attacchi di tipo chosen plain-text, perché conosco la chiave pubblica

Scelgo un numero qualsiasi di messaggi in chiaro, costruisce i crittogrammi relativi e ascolta sul canale confrontando i crittogrammi in transito e se trova un riscontro sa esattamente qual è il messaggio passato.

**Come si usa** Oggi si usa un cifrario a chiave segreta (AES) per le comunicazioni di massa, e un cifrario a chiave pubblica per scambiare le chiavi segrete relative al primo senza incontri fisici tra gli utenti.

Diventa lento solo lo scambio delle chiavi. Siamo anche al sicuro da attacchi chosen plain-text perché se la chiave è scelta bene risulta imprevedibile dal crittoanalista.

## 1.3 Rappresentazione matematica di oggetti

Per rappresentare gli oggetti scegliamo dei **caratteri** da un **insieme finito** detto **alfabeto**.

Un **oggetto** è **rappresentato da una sequenza ordinata di caratteri dell'alfabeto**. L'ordine dei caratteri è importante: a **oggetti diversi corrispondono sequenze diverse** e **il numero di oggetti che si possono rappresentare non ha limiti**. Significa che fissando un numero  $n$  arbitrariamente grande possiamo sempre creare un numero di oggetti  $> n$ , con sequenze via via più grande.

**Alfabeto**  $\Gamma$  con  $|\Gamma| = s$  e  $N$  oggetti da rappresentare.

$d(s, N)$ : lunghezza della sequenza più lunga che rappresenta un oggetto dell'insieme. A noi interessa la rappresentazione che minimizza  $d(s, N)$ , cioè  $d_{min}(s, N)$

Una rappresentazione è tanto più efficiente quanto  $d(s, N)$  si avvicina a  $d_{min}(s, N)$

**Esempio**  $s = 1, \Gamma = \{0\}$  l'unica possibilità è variare la lunghezza  $\Rightarrow d_{\min}(1, N) = N$ , estremamente sfavorevole.  
 $s = 2, \Gamma = \{0, 1\}, \forall k \geq 1$  ho  $2^k$  sequenze di lunghezza  $k$ . Il numero totale di sequenze lunghe da 1 a  $k$  è  $2^{k+1} - 2$  (si esclude anche la sequenza nulla). Con  $N$  oggetti da rappresentare  $\Rightarrow k \geq \log_2(N+2) - 1 \Rightarrow N$  sequenze diverse tutte di  $\log_2(N)$  caratteri.

**Efficiente** Codifica efficiente quando c'è questa riduzione logaritmica, **efficiente** quando . Sequenze della stessa lunghezza è vantaggioso perché non servono caratteri separatori. Per questo è necessario che l'alfabeto contenga almeno due caratteri.

La **notazione posizionale** è una rappresentazione efficiente indipendentemente dalla base  $s \geq 2$  scelta. Un intero  $N$  è rappresentato con un numero  $d$  di cifre  $\lfloor \log_s(N) \rfloor \leq d \leq \log_s(N) + 1$

## 1.4 Richiamo della teoria della calcolabilità

**Problemi computazionali** Formulati matematicamente di cui cerchiamo una soluzione algoritmica: **decidibili** (e **trattabili** o **non trattabili**), o **non decidibili**.

Calcolabilità  $\rightarrow$  **Algoritmo** e **problema non decidibile**

Complessità  $\rightarrow$  **Algoritmo efficiente** e **problema intrattabile**.

**Numerabilità** Due insiemi  $A$  e  $B$  hanno lo stesso numero di elementi  $\Leftrightarrow$  si può stabilire una **corrispondenza biunivoca** tra i loro elementi.

Questo porta alla definizione di **numerabile**: un insieme è numerabile  $\Leftrightarrow$  i suoi elementi possono essere messi in **corrispondenza biunivoca con i numeri naturali**.

Numerabile significa che **possiede un'infinità numerabile di elementi**. Esempi: l'insieme dei numeri naturali  $N$ , l'insieme degli interi  $Z$  (avendo  $n$  in corrispondenza biunivoca con  $2n+1$  per  $n \geq 0$  e  $n \leftrightarrow 2|n|$  per  $n < 0$ , dando la sequenza  $0, -1, 1, -2, 2, \dots$ ) o anche l'insieme dei naturali pari ( $2n \leftrightarrow n$ )

**Enumerazione delle sequenze** Si vuole elencare in uno ordine ragionevole le sequenze di lunghezza finita costruite su un alfabeto finito. Le sequenze non sono in numero finito, quindi non si potrà completare l'elenco.

Lo scopo è **raggiungere qualsiasi sequenza  $\sigma$  arbitrariamente scelta in un numero finito di passi**.  $\sigma$  deve dunque trovarsi a **distanza finita** dall'inizio dell'elenco. Non va bene l'ordine del dizionario perché non saprei la posizione della prima stringa che inizia con  $b$  perché le stringhe composte da tutte  $a$  sono infinite.

Si stabilisce un ordine tra i caratteri. Si ordinano prima in lunghezza crescente e, a pari lunghezza, in ordine alfabetico.

**Esempio**  $\Gamma = \{a, b, \dots, z\}$ , avrei

$a, b, \dots, z,$

$aa, ab, \dots, az, ba, bb, \dots, bz, \dots, zz, \dots$

Ad una sequenza arbitraria corrisponde un numero intero, e la sequenza  $s$  arbitraria si troverà tra quelle di lunghezza  $|s|$  in posizione alfabetica. Quindi ad una sequenza arbitraria  $\leftrightarrow n$  che indica la posizione nell'elenco, e ad un numero naturale  $n \leftrightarrow$  la sequenza che occupa l' $n$ -esima posizione nell'elenco.

La **numerazione delle sequenze è fattibile perché sono di lunghezza finita**, anche se illimitata. Cioè per qualunque intero  $d$  scelto a priori, esistono sequenze di lunghezza maggiore di  $d$ . Per sequenze di lunghezza infinita la numerazione non è possibile

**Insiemi non numerabili** Insiemi non equivalenti a  $N$  come  $R, (0, 1)$ , l'insieme di tutte le linee del piano, insieme delle funzioni in una o più variabili.  $\dots \Rightarrow$  **l'insieme dei problemi computazionali non è numerabile**. Perché un problema computazionale è sempre visualizzabile come una funziona matematica, che associa ad ogni insieme di dati espressi da  $k$  numeri interi il corrispondente risultato espresso da  $j$  numeri interi

$$f : N^k \rightarrow N^j$$

Quindi l'insieme di queste  $f$  **non è numerabile**.

**Diagonalizzazione**  $F = \{ \text{funzioni } f \mid f : N \rightarrow \{0, 1\} \}$ , ogni  $f \in F$  è rappresentata da una sequenza infinita

$x \ 0 \ 1 \ 2 \ 3 \ \dots n \ \dots$

$f(x) \ 0 \ 1 \ 0 \ 1 \ \dots 0 \ \dots$

ma se è possibile è rappresentabile con una regola (f 0 se x pari 1 se x dispari)

Per assurdo, ipotizzo  $F$  numerabile. Si può assegnare ad ogni funzione un numero progressivo nella numerazione e costruire una tabella infinita con tutte le funzioni.

$x$	0	1	2	3	4	5	6	7	8	...
$f_0(x)$	1	0	1	0	1	0	0	0	1	...
$f_1(x)$	0	0	1	1	0	0	1	1	0	...
$f_2(x)$	1	1	0	1	0	1	0	0	1	...
$f_3(x)$	0	1	1	0	1	0	1	1	1	...
$f_4(x)$	1	1	0	0	1	0	0	0	1	...

Definisco  $g(x) = \begin{cases} 0 & f_x(x) = 1 \\ 1 & f_x(x) = 0 \end{cases} \Rightarrow g$  non può corrispondere a nessuna delle  $f_i$  della tabella, perché differisce da tutte le funzioni almeno nella diagonale principale.

$g(x) \mid 0111\dots$

Per assurdo  $\exists j \mid g(x) = f_j(x) \Rightarrow g(j) = f_j(j)$  ma per la definizione  $g(j)$  è il complemento di  $f_j(j)$ , quindi  $g(j) \neq f_j(j)$   
**contraddizione.**

Per qualunque numerazione scelta esiste sempre almeno una funzione esclusa, quindi  $F$  non è numerabile.

### 1.4.1 Algoritmi

**Algoritmi** la **formulazione di un algoritmo**, una sequenza finita di operazioni, completamente e univocamente determinate, **dipende dal modello di calcolo utilizzato.**

Qualunque modello si scelga, gli algoritmi devono essere descritti da sequenze finite di caratteri di un alfabeto finito  
 $\Rightarrow$  sono **possibilmente infiniti ma numerabili.**

**Problemi computazionali** Sono **funzioni matematiche** che associano ad ogni insieme di dati il corrispondente risultato, e **non sono numerabili** come visto prima.

**Problema della rappresentazione** C'è una drastica perdita di potenza, perché gli algoritmi sono numerabili ma sono meno dei problemi computazionali

$$|\{Problemi\}| \gg |\{Algoritmi\}|$$

$\Rightarrow$  **esistono problemi privi di un corrispondente algoritmo di calcolo.** Per esempio, il problema dell'arresto.

**Lezione di Turing** *Non esistono algoritmi che decidono il comportamento di altri algoritmi esaminandoli dall'esterno, cioè senza passare dalla loro simulazione.*

### 1.4.2 Modelli di calcolo

La teoria della calcolabilità dipende dal modello di calcolo?

Oppure

la decidibilità è una proprietà del problema?

I linguaggi di programmazione esistenti sono tutti equivalenti?

Ce ne sono di alcuni più potenti/più semplici di altri?

Ci sono algoritmi descrivibili in un linguaggio ma non in un altro?

È possibile che problemi oggi irrisolvibili possano essere risolti in futuro con altri linguaggi o altri calcolatori?

Le teorie della calcolabilità e della complessità dipendono dal modello di calcolo?

**Tesi di Church-Turing** Tutti i *ragionevoli* modelli di calcolo **risolvono esattamente la stessa classe di problemi**, quindi **si equivalgono nella possibilità di risolvere i problemi** pur operando con diversa efficienza.

**Tesi C-H: la decidibilità è una proprietà del problema**

Incrementi qualitativi sui calcolatori o sui linguaggi di programmazione servono **solo** ad abbassare i tempi di esecuzione o rendere più agevole la programmazione.

### 1.4.3 Decidibilità e trattabilità

Ci sono quindi problemi che non possono essere risolti da nessun calcolatore, indipendentemente dal tempo impiegato (**problemi indecidibili**).

Ci sono poi problemi decidibili che possono richiedere tempi di risoluzione esponenziali nella dimensione dell'istanza (**problemi intrattabili**).

Ci sono poi problemi che possono essere risolti con algoritmi di costo polinomiale nella dimensione dell'input (**problemi trattabili**).

Abbiamo poi una famiglia di problemi il cui stato non è noto: clique (cricca), cammino hamiltoniano... Sappiamo risolverli (decidibili) con algoritmi di costo esponenziale, ma non abbiamo limiti inferiori esponenziali. I migliori limiti inferiori sono polinomiali: c'è un gap fra il limite inferiore (polinomiale) e costo della migliore soluzione a disposizione (esponenziale) (**presumibilmente intrattabili**).

#### Notazione

Studiamo la dimensione dei dati trattabili in funzione dell'incremento della velocità dei calcolatori.

Dati i calcolatori  $C_1$ ,  $C_2$  ( $k$  volte più veloce di  $C_1$ ) e tempo di calcolo a disposizione  $t$ , avrò  $n_1$  dati trattabili in tempo  $t$  su  $C_1$  e  $n_2$  trattabili in tempo  $t$  su  $C_2$ .

Si osserva che **usare  $C_2$  per un tempo  $t$  equivale a usare  $C_1$  per un tempo  $k \cdot t$** .

**Algoritmi polinomiali** Un algoritmo polinomiale che risolve il problema in  $c \cdot n^s$  secondi, con  $c$  ed  $s$  costanti.

$$C_1 \quad c \cdot n_1^s = t \Rightarrow n_1 = (t/c)^{1/s}$$

$$C_2 \quad c \cdot n_2^s = t \Rightarrow n_2 = k^{1/s} \cdot (t/c)^{1/s}$$

$$\Rightarrow n_2 = k^{1/s} \cdot n_1, \text{ miglioramento di un fattore } \mathbf{moltiplicativo} \quad k^{1/s}$$

**Algoritmi esponenziali** Un algoritmo polinomiale che risolve il problema in  $c \cdot 2^n$  secondi, con  $c$  costante.

$$C_1 \quad c 2^{n_1} = t \Rightarrow 2^{n_1} = t/c$$

$$C_2 \quad c 2^{n_2} = k \cdot t \Rightarrow 2^{n_2} = k \cdot t/c = k 2^{n_1}$$

$$\Rightarrow n_2 = n_1 + \log_2(k), \text{ miglioramento di un fattore } \mathbf{additivo} \quad \log_2(k)$$

Di conseguenza **un algoritmo efficiente è di gran lunga più importante di un calcolatore più potente**.

### 1.4.4 Tipologie di problemi

Dato un problema  $\Pi$  su un insieme di istanze in ingresso  $I$  con un insieme di soluzioni  $S$ .

**Problemi decisionali** Richiedono una risposta binaria  $S = \{0, 1\}$ , quindi istanze positive  $x \in I \mid \Pi(x) = 1$  o negative  $x \in I \mid \Pi(x) = 0$ . Esempio: verifica se un numero è primo, o se un grafo è connesso.

La teoria della complessità computazionale è definita principalmente in termini di problemi di decisione: risposta binaria, quindi il tempo per restituire la risposta è costante, e la complessità di un problema è già presente nella versione decisionale.

**Problemi di ricerca** Data un'istanza  $x$ , richiede di restituire una soluzione  $s$ .

**Problemi di ottimizzazione** Data un'istanza  $x$ , si vuole trovare la **migliore** soluzione  $s$  tra tutte quelle possibili. Esempio: clique di dimensione massima, cammino minimo...

### 1.4.5 Classi di complessità

Dato un problema **decisionale**  $\Pi$  ed un algoritmo  $A$ , diciamo che  $A$  **risolve**  $\Pi$  se, data un'istanza di input  $x$ ,  $A(x) = 1 \Leftrightarrow \Pi(x) = 1$

$A$  risolve  $\Pi$  in **tempo**  $t(n)$  e **spazio**  $s(n)$ .

#### Classi Time e Space

$\text{Time}(f(n))$ : insieme dei **problemi decisionali che possono essere risolti in tempo**  $O(f(n))$

$\text{Space}(f(n))$ : insieme dei **problemi decisionali che possono essere risolti in spazio**  $O(f(n))$

**Classe P** Classe dei problemi risolvibili in **tempo** polinomiale nella dimensione dell'istanza di input.

**Algoritmo polinomiale** nel tempo:  $\exists c, n_0 > 0 \mid$  il numero di passi elementari è al più  $n^c$  per ogni input di dimensione  $n > n_0$ .

**Classe PSPACE** Classe dei problemi risolvibili in **spazio** polinomiale nella dimensione dell'istanza di input. Molto più grande di P.

**Algoritmo polinomiale** nello spazio:  $\exists c, n_0 > 0 \mid$  il numero di celle di memoria è al più  $n^c$  per ogni input di dimensione  $n > n_0$ .

**Classe EXPTIME** Classe dei problemi risolvibili in tempo esponenziale nella dimensione dell'istanza di input.

$$P \subseteq PSPACE \subseteq EXPTIME$$

Non è noto se queste inclusioni siano note, ad oggi. L'unico risultato dimostrato finora riguarda P ed EXPTIME: esiste un problema che può essere risolto in tempo esponenziale ma per cui il tempo polinomiale non è sufficiente (es: torri di Hanoi).

### 1.4.6 Certificato

Per alcuni problemi, per le istanze accettabili (istanze in cui la risposta del problema decisionale è sì), è possibile certificare che quell'istanza è accettabile con un certificato  $y$  che può convincerci dell'accettabilità.

Per clique, il certificato è il sottoinsieme di  $k$  vertici che forma la clique. Per il cammino hamiltoniano è la permutazione degli  $n$  vertici che formano il cammino. Per SAT, sono le assegnazioni che rendono vera la formula. Il certificato ha dimensione polinomiale ( $k, n$ ) e la verifica del certificato è lineare.

Una volta che ho il certificato lo vado a verificare: attestato breve di esistenza di una soluzione con determinate proprietà. Si definisce solo per istanze accettabili, perché spesso la non accettabilità non è facile costruire un certificato.

**Idea** Usare il costo della verifica di un certificato per un'istanza accettabile per **caratterizzare la complessità del problema** stesso.

Un problema è **verificabile in tempo polinomiale** se: tutte le istanze accettabili ammettono un certificato di lunghezza polinomiale ed esiste un algoritmo di verifica polinomiale in  $n$ .

**Classe NP** Classe dei problemi decisionali **verificabili in tempo polinomiale**. (NP = polinomiale su macchine non deterministiche)

**P  $\subset$  NP?** Ovviamente sì, ogni problema in P ammette un certificato verificabile in tempo polinomiale: eseguo l'algoritmo che risolve il problema per costruire il certificato.

Quello che non sappiamo è  $P = NP$  oppure  $P \neq NP$ . Si pensa  $P \neq NP$ .

Si possono individuare i problemi più difficili in NP, ovvero quelli candidati ad appartenere ad NP se  $P \neq NP$ : sono i problemi NP-completi, quelli per cui se esiste un algoritmo polinomiale per risolvere un NP-completo allora tutti i problemi NP potrebbero essere risolti in tempo polinomiale e quindi  $P = NP$ .

Quindi tutti i problemi NP-completi sono risolvibili in tempo polinomiale oppure nessuno lo è.

Tutti i problemi NP-completi possono essere ridotti l'un l'altro, sono NP-equivalenti.

## Gerarchia delle classi secondo le attuali congetture



La fattorizzazione ad esempio  $\in NP - (P \cup NP\text{completi})$ , infatti è risolto in tempo polinomiale su macchine quantistiche.

## 1.4.7 Classi co-P e co-NP

C'è molta differenza tra certificare l'esistenza e certificare la non esistenza di una soluzione. Dato un problema  $\Pi$  possiamo definire  $\text{co}\Pi$  che accetta tutte e sole le istanze rifiutate da  $\Pi$ .

La classe  $\text{co}P$  è la classe per cui  $\text{co}\Pi \in P$ .  $P = \text{co}P$ , i problemi complementari e i co-complementari (originali) si possono entrambi risolvere in tempo polinomiale: risolvo il problema complementare e complemento il risultato.

Questo non vale per  $\text{co}NP$ , la classe per cui  $\text{co}\Pi \in NP$ . Si congettura che siano diverse, se la congettura è vera allora  $P \neq NP$







## Capitolo 2

# Sequenze Casuali

### 2.1 Esempi di algoritmi numerici

**Algoritmo di Euclide** Algoritmo per il calcolo dell'MCD fra due interi.

Suppongo due interi  $a, b$  con  $a \geq b$ ,  $a > 0$  e  $b \geq 0$

$$\text{MCD}(a, b) = \begin{cases} a & b = 0 \\ \text{MCD}(a, a \bmod b) & \text{else} \end{cases}$$

**Valutazione complessità** Data l'istanza di input composta da  $a, b$ , vengono rappresentati ad esempio in base due. Quindi la dimensione  $n$  dell'istanza di input  $|I| = \Theta(\log a + \log b) = \Theta(\log a)$ .

L'algoritmo è ricorsivo, quindi bisogna valutare il numero delle chiamate ricorsive, che dipenderanno dai dati. Ci saranno istanze in cui si termina subito (ad esempio se  $a$  multiplo di  $b$ , cioè  $a \bmod b = 0$ ). In generale, **il numero di chiamate cresce con  $\log a$** , perché  $a \bmod b$  rimpiazza  $a$ .

Si osserva che  $a \bmod b < \frac{a}{2}$

Questo perché  $a = qb + (a \bmod b)$  e siccome per ipotesi  $a \geq b \Rightarrow b \geq 1$  e lo è anche  $q \Rightarrow a \geq b + (a \bmod b) > (a \bmod b) + (a \bmod b)$  perché  $b > (a \bmod b)$ .

$\Rightarrow 2(a \bmod b) < a \Rightarrow (a \bmod b) < \frac{a}{2}$ .

Prima chiamata su  $a, b$ .

Seconda su  $b, (a \bmod b)$ .

Terza su  $(a \bmod b), (b \bmod (a \bmod b))$ .

Quindi ad ogni chiamata si riduce almeno della metà, e lo possiamo fare al massimo  $\log a$  volte

**Quindi avrò  $O(\log a)$  ricorsioni.**

Il costo del calcolo del modulo è  $O(\log a \cdot \log b) = O(\log^2 a)$

Complessivamente  $T(n) = O(\log^3 a) = O(n^3)$  **polinomiale nella dimensione dell'istanza  $|I|$**  (cioè nel numero di cifre), **polilogaritmico nel valore dei dati**

**Test di primalità** Versione inefficiente.

Primo(N): **for** ( $i = 2, i \leq \sqrt{N}, i++$ )

**if**  $N \% i == 0$  **return false**

**else a fine ciclo return true.**

Uso la proprietà che se  $N$  non è primo allora ha almeno un divisore  $\leq \sqrt{N}$ .

**Valutazione di complessità**  $I = N, |I| = \Theta(N) = n$

Ho  $\sqrt{N}$  iterazioni, ciascuna di costo  $\Theta(\log^2 N)$

$T(n) = O(\sqrt{N} \cdot \log^2 N) = O(2^{\frac{n}{2}} \cdot n^2)$  **pseudopolinomiale**, cioè **polinomiale nel valore di  $N$  ma esponenziale nella dimensione  $|I| = n$ .**

## 2.2 Casualità

**Problema** Data una sequenza binaria, vogliamo **capire se è una sequenza casuale** o meno. Le sequenze casuali sono importanti sia per la generazione delle classi, sia perché **in crittografia spesso si ricorrono ad algoritmi randomizzati che usano sequenze casuali per funzionare.**

**Significato algoritmico della casualità** Vedendo la teoria di Kolmogorov. Prendiamo due sequenze

$h$ : 1111...1 lunga  $n$

$h'$ : 10110110101011010100101...0

**La prima è molto facile da descrivere** (*scrivi  $n$  "uni"*), mentre **descrivere la seconda è molto meno pratico**: l'intuizione è che **una sequenza casuale non si può descrivere in modo compatto.**

Ponendo  $n = 20$ , la probabilità di generare  $h$  è  $P(h) = (1/20)^{20}$ ,  $P(h') = (1/20)^{20}$  (1/2 per generare 1, 1/2 per generare 0...).

$A_h$  algoritmo che genera  $h$ . Formalizzabile semplicemente (*genera  $n$  uni*)

$|A_h| = \# \text{ bit di } A_h \text{ codificato in binario} = \log n + \text{const}$  (la parte costante è la generazione e l'output, varia solo  $n$ )  $\Rightarrow$  con  $\log n$  bit ne abbiamo descritti  $n$ .

$A_{h'} = \text{print } h', |A_{h'}| > |n| = |h'|$

L'intuizione è **una sequenza binaria è casuale se non ammette un algoritmo di generazione la cui rappresentazione binaria sia più corta di  $h$ .** Se posso usare meno bit vuol dire che la sequenza ha una qualche regolarità.

**Sistemi di calcolo** Sono un'infinità numerabile  $S_1 \dots S_i \dots$

Prendiamo  $S_i$ ,  $p$  programma che genera la sequenza  $h$  nel sistema  $S_i$ , cioè  $S_i(p) = h$

**Def: la complessità di Kolmogorov di  $h$  nel sistema  $S_i$  è  $K_{S_i}(h) = \min\{|p| \mid S_i(p) = h\}$**  cioè la minima lunghezza del programma  $p$  che in  $S_i$  genera  $h$  stessa.

Se la sequenza  $h$  non segue alcuna legge semplice di regolarità, allora **il più breve programma in grado di generarla dovrà contenerla al suo interno**, cioè sarà almeno lungo quanto la sequenza stessa e la genererà trasferendola in output. Quindi  $K_{S_i}(h) = |h| + \text{const}_i$ . La costante è la parte di programma che trasferisce in output, dipende da  $S_i$  ma non ha  $h$ .

**Sistema di calcolo universale** Tra tutti i sistemi di calcolo possibili ne esiste uno **universale in grado di simulare tutti gli altri**. Lo chiamiamo  $S_u$  e lo prendiamo in considerazione.

Supponiamo  $p \mid S_i(p) = h$ , allora  $S_u(\langle i, p \rangle) = S_i(p) = h$ . Ottengo  $q = \langle i, p \rangle$  programma che genera  $h$  in  $S_u$

$|q| = |\langle i, p \rangle| = |i| + |p| = \log_2 i + |p|$  quindi la lunghezza di  $q$  dipende da  $i$  ma non da  $h$ .

$\forall h \forall i K_{S_u}(h) \leq K_{S_i}(h) + C_i$

L'uguale vale per le sequenze generate per simulazione di  $S_i$  non essendoci per  $S_u$  algoritmi più "brevi".

Il minore vale per sequenze generabili con programmi più corti (ad esempio per simulazione su un altro sistema  $S_j \neq S_i$ ).

**Def** La complessità di Kolmogorov di una sequenza  $h$  è  $K(h) = K_{S_u}(h)$

### 2.2.1 Sequenze casuali

**Sequenza casuale** Una sequenza  $h$  è casuale se  $K(h) \geq |h| - \lceil \log_2 h \rceil$

Non entra in gioco come genero la sequenza, la **casualità è una proprietà della sequenza.**

**Conteggio delle sequenze**  $\forall n, \exists$  sequenze casuali (secondo Kolmogorov) di lunghezza  $n$

**Dim:**  $n, S = 2^n$  # sequenze binarie di lunghezza  $n$

$T = \#$  sequenze di lunghezza  $n$  NON casuali. L'obiettivo è dimostrare che  $T < S$ .

Pongo  $N = \#$  sequenze binarie di lunghezza  $< n - \lceil \log_2 n \rceil = \sum_{i=0}^{n-\lceil \log_2 n \rceil - 1} 2^i = 2^{n-\lceil \log_2 n \rceil} - 1$

Tra queste  $N$  sequenze ci sono anche i programmi che generano le  $T$  sequenze non casuali di lunghezza  $n$ .

$\Rightarrow T \leq N < S \Rightarrow T < S$

Quindi non solo esistono ma sono anche la **maggioranza**, essendo enormemente più numerose di quelle non casuali. Lo vediamo studiando il rapporto

$$\frac{T}{S} \leq \frac{N}{S} = \frac{2^{n-\lceil \log n \rceil}}{2^n} - \frac{1}{2^n} < \frac{1}{2^{\lceil \log n \rceil}} \quad \lim_{n \rightarrow +\infty} \frac{T}{S} = 0$$

**Stabilire la casualità** Data una sequenza arbitraria di lunghezza  $n$ , stabilire se è casuale secondo Kolmogorov è un problema **indecidibile**.

**Dim:** per assurdo suppongo esista un algoritmo  $\text{Random} \mid \text{Random}(h) = \begin{cases} 1 & h \text{ casuale} \\ 0 & \text{altrimenti} \end{cases}$

Possiamo costruire l'algoritmo Paradosso che enumera tutte le possibili sequenze binarie in ordine crescente di lunghezza.

Paradosso:

```
for (binary h = 1 → infity) do
  if (|h| - ⌈log |h|⌉ > |P| && Random(h) == 1) return h
```

$P$  è una sequenza binaria che rappresenta la codifica del programma complessivo Paradosso + Random, quindi  $|P| = |\text{Paradosso}| + |\text{Random}|$ , costante che non dipende da  $h$ , perché la sequenza  $h$  non compare in  $P$  ma solo come nome di variabile. Il valore rimane registrato fuori dal programma.

**Paradosso quindi restituisce come risultato la prima sequenza casuale**  $|h| - \lceil \log_2 |h| \rceil > |P|$

Quindi se  $\exists$  sequenze casuali di qualsiasi lunghezza, quindi certamente ne esisterà una che soddisfa entrambe le condizioni dell'**if**, che viene generata.

Ma la prima condizione mi dice che il programma rappresentato da  $P$  è breve e genera  $h$ , quindi  $h$  non è casuale perché prodotta con un programma breve.

Quindi  $K(h) \leq |P|$ , cioè  $P$  genera  $h$  ma  $|P| < |h| \lceil \log_2 |h| \rceil$  quindi  $h$  non è casuale.

Ma la seconda condizione dice  $h$  casuale, giungendo ad un **paradosso** dato dall'assumere l'esistenza di Random.

### 2.2.2 Sorgente binaria casuale

**Generatore** Genera una sequenza di bit con queste proprietà:

1.  $P(0) = P(1) = 1/2$ , cioè genera 1 o 0 a pari probabilità.  
Si può indebolire richiedendo  $P(0) > 0$ ,  $P(1) > 0$  immutabili nel tempo della generazione.
2. La generazione di un bit è indipendente dalla generazione degli altri.  
 $\Rightarrow$  non si può prevedere il valore di un bit osservando quelli già generati.

Perché possiamo indebolire la prima proprietà? Supponiamo di essere in un caso in cui  $P(0) > P(1)$ , allora è **sempre possibile bilanciare la sequenza**.

Supponiamo di generare 001100111000010100 e si **dividono a coppie** 00 11 00 11 10 00 01 01 00 e si scartano le coppie uguali. Si associano le coppie miste, ad esempio 01  $\rightarrow$  0 e 10  $\rightarrow$  1. Si presentano in modo equiprobabile, quindi la sequenza si ribilancia ottenendo 100 (caso poco significativo perché sequenza corta).

**Esistono queste sorgenti?** Non si sa. Nella pratica non è possibile garantire la perfetta casualità o l'indipendenza. Quindi sfrutteremo le casualità presenti in processi fisici o processi software.

#### Generatore di sequenze brevi

**Fenomeni casuali presenti in natura** Ad esempio il rumore su un microfono o il tempo di decadimento di alcune particelle, sfruttabili come sorgenti di casualità.

Il problema di questo approccio è che bisogna non avere accesso fisico ai dispositivi usati (es: microfono manomesso), oltre alla difficoltà pratica di usare certe sorgenti.

**Processi software** Come la temperatura, la posizione della testina del disco fisico...

**Pseudocasuale** Si genera la casualità **mediante un algoritmo, cercandola all'interno di processi matematici**. **Generatore di numeri pseudo-casuali:** ad esempio `rand()` del C.

Perché pseudocasuali? Perché sono algoritmi deterministici e brevi, quindi non risultano casuali secondo Kolmogorov.

**Come funzionano?** Partono da un *seed* (seme), breve sequenza che viene amplificata per creare una sequenza più lunga. Quindi un generatore è un **amplificatore di casualità**.

Input: seme (sequenza o valore breve)

Output: flusso di bit arbitrariamente lungo e periodico.

Al suo interno contiene una sottosequenza che si **ripete**, quindi **un generatore è tanto migliore tanto più è lungo il suo periodo**

Avengo  $s = \#$  bit nel seme e  $n$  lunghezza della sequenza ottenuta dal generatore, con  $n \gg s$ , ho **una sequenza diversa per ogni seme**, con  $2^s$  possibili semi.

$\#$  sequenze diverse  $2^s \ll 2^n$   $\#$  sequenze possibili

**Generatore lineare**  $x_i = (a \cdot x_{i-1} + b) \bmod n$  con  $a, b, n$  interi positivi.

Il seme è un valore intero iniziale casuale  $x_0$ , quindi quando  $x_i = x_0$  la sequenza si ripete.

Dobbiamo avere  $\text{MCD}(b, n) = 1$ ,  $(a - 1)$  divisibile per ogni fattore primo di  $n$  e  $(a - 1)$  dev'essere un multiplo di 4 se anche  $n$  lo è.

Servono per garantire che il generatore produca una permutazione degli interi da 0 a  $m - 1$

## 2.3 Test statistici

Per valutare le sequenze prodotte da un generatore pseudocasuale.

Si valuta se la sequenza presenta le proprietà tipiche di una sequenza casuale:

**test di frequenza**

**poker test:** se sottosequenze siano distribuite in modo equo

**test di autocorrelazione:** verifica che non ci siano regolarità nella sequenza ottenuta

**run test:** verifica se sottosequenze massimali di elementi tutti ripetuti abbiano una distribuzione esponenziale negativa, cioè più sono lunghe meno sono frequenti.

Per le applicazioni crittografiche si richiede anche il **test di prossimo bit**, molto severo che implica tutti gli altri 4 test statistici. Intuitivamente, verifica che sia impossibile prevedere gli elementi della sequenza prima di generarli.

**Test di prossimo bit** Un generatore binario **supera** il test di prossimo bit **se non esiste un algoritmo polinomiale in grado di prevedere l' $i + 1$ -esimo bit della sequenza a partire dalla conoscenza degli  $i$  bit precedentemente generati con probabilità maggiore di  $1/2$ .**

Quindi se si hanno a disposizione risorse polinomiale non si può prevedere il prossimo bit. I generatori che superano questo test sono detti **generatori crittograficamente sicuri**.

**Generatore polinomiale** Non è crittograficamente sicuro.

$$x_i = (a_1 x_{i-1}^t + a_2 x_{i-1}^{t-1} + \dots + a_t x_{i-1} + a_{t-1}) \bmod n$$

$$r_i = \frac{x_i}{n}$$

## 2.4 Generatori crittograficamente sicuri

**Come costruire generatori crittograficamente sicuri** Si ricorre alle **funzioni one-way**: funzioni facili da calcolare ma difficili da invertire, cioè **computabili in tempo polinomiale** ( $x \mapsto f(x)$ ), ma **computazionalmente difficile invertire la funzione** ( $y \mapsto x = f^{-1}(y)$ ). Come costruire queste funzioni?

**Idea** Con  $f$  one-way, scelgo il seme  $x_0$ . Genero  $S: x \ f(x) \ f(x_1) = f(f(x)) \dots x_i = f(f(\dots(x_{i-1})\dots))$

Cioè si itera l'applicazione della funzione one-way un numero arbitrario di volte. **L'idea è restituire la sequenza al contrario**, perché se conosco  $x_{i+1}$  non riesco a calcolare facilmente  $x_i$ .

Ogni elemento della sequenza  $S$  si può calcolare efficientemente con l'elemento precedente, ma non dai valori successivi perché  $f$  è one-way. Si calcola  $S$  per un certo numero di passi senza svelare il risultato e si comunicano gli elementi in ordine inverso. Ogni elemento non è prevedibile in tempo polinomiale pur conoscendo quelli comunicati.

**Generatori binari crittograficamente sicuri** Si usano i "predicati *hard core*" delle funzioni one-way.

Un predicato hard core di una funzione one-way  $f(x)$  è  $b(x)$  se  $b(x)$  è facile da calcolare quando  $x$  è noto, ma è difficile da prevedere se si conosce  $f(x)$ .

Un esempio di funzione one-way è l'elevamento a quadrato in modulo ( $f(x) = x^2 \bmod n$  con  $n$  non primo). Un predicato hard core è " $b(x) = x$  è dispari"

**Generatore BBS** Crittograficamente sicuro.

$n = p \cdot q$ , con  $p$  e  $q$  primi grandi.

$$p \bmod 4 = 3$$

$$q \bmod 4 = 3$$

$$2\lfloor \frac{p}{4} \rfloor + 1 \text{ e } 2\lfloor \frac{q}{4} \rfloor + 1 \text{ primi fra loro}$$

$\Rightarrow y$  coprimo con  $n$ , si calcola  $x_0 = y^2 \bmod n$  e si usa come seme per calcolare una successione di  $m \leq n$  interi

$$x_i = (x_{i-1})^2 \bmod n$$

$$b_i = 1 \Leftrightarrow x_{n-i} \text{ è dispari}$$

$$b_1 = 1 \Leftrightarrow x_{n-1} \text{ dispari}$$

$$b_0 = 1 \Leftrightarrow x_n \text{ dispari}$$

Quindi  $x_0 = b_n$ , ottengo una sequenza del tipo

$$x_0 \rightarrow x_1 \rightarrow \dots \rightarrow x_{n-1} \rightarrow x_n$$

$$\Rightarrow b_n \rightarrow b_{n-1} \rightarrow \dots \rightarrow b_1 \rightarrow b_0$$

La sequenza viene restituita in ordine inverso  $b_0 b_1 \dots$

### 2.4.1 Generatori di numeri pseudocasuali basati su cifrari simmetrici

**Idea** Prendere un cifrario simmetrico e la sua chiave. Anziché usarlo per costruire un crittogramma, si sostituisce il messaggio da cifrare con un **seme iniziale** legato al generatore. Si comincia a cifrare in questo modo: produce una sequenza imprevedibile per le proprietà del cifrario.

Di seguito, un esempio approvato dal FIPS:

Usa il DES

$r = \#$  bit delle parole che vengono prodotte  
( $r = 64$  nel DES)

$s =$  seme casuale di  $r$  bit

$m = \#$  parole da produrre

$k =$  chiave segreta del cifrario

```

Generatore(s, m){ //flusso di output di m*r bit
    d = <rapp. su r bit di data e ora>;
    y = C(d, k);
    z = s;
    for (i = 1; i <= m; i++) {
        xi = C(y xor z, k);
        z = C(y xor xi, k);
        output(xi);
    }
}

```

## 2.5 Algoritmi randomizzati

Si dividono in due classi fondamentali:

**Algoritmi Las Vegas**

Generano un **risultato sicuramente corretto** in un **tempo probabilmente breve**.

Caso tipico: quick sort. Qualche passo a caso per cercare di evitare i casi sfavorevoli.

**Algoritmi Montecarlo**

Generano un **risultato probabilmente corretto** in un **tempo sicuramente breve**.

**Probabilità di errore** deve essere **arbitrariamente piccola e matematicamente misurabile**.

Caso tipico: test di primalità.

### 2.5.1 Test di primalità (Miller, Rabin)

$N$  intero (dispari) da testare di  $n$  bit

$\Rightarrow N-1$  è pari,  $N-1 = 2^w \cdot z$  con  $z$  dispari,  $w$  esponente della potenza di 2 più grande che divide  $N-1$

Es:  $N = 21$ ,  $N-1 = 20 = 2^2 \cdot 5$  quindi  $z = 5, w = 2$

Da  $N$ , calcolo  $N-1 \rightarrow \frac{N-1}{2} \rightarrow \frac{N-1}{4} \rightarrow \dots \rightarrow z = 1$  quindi # divisioni per  $2 \leq \log N = n$  volte

Quindi trovo  $w$  e  $z$  in maniera efficiente,  $O(n)$  passi

Sia quindi  $N$  primo e  $2 \leq y \leq N-1$  arbitrario detto *testimone*, allora

P1  $\text{MCD}(N, y) = 1$ , per la primalità

P2  $(y^z \bmod N = 1) \vee (\exists i \ 0 \leq i \leq w-1 \mid y^{2^i \cdot z} \bmod N = -1)$

Se una delle due proposizione è falsa allora  $N$  non è primo, ma ci sono numeri composti che verificano P1 e P2 ma non sono primi (sono pochi).

**Lemma 1** (Miller, Rabin)  $N$  è composto, allora il numero di testimoni  $y$  che soddisfano i predicati è basso. Cioè  $N$  composto  $\Rightarrow$  il numero di interi  $y \mid 2 \leq y \leq N-1$  che soddisfano entrambi i predicati P1 e P2 è minore di  $N/4$ . La probabilità di scegliere un testimone che rende veri P1 e P2  $< \frac{N/4}{N-2} < \frac{1}{4}$

$N$   $y$  scelto a caso in  $[2, N-1]$ :

se uno dei due predicati è **falso**  $\rightarrow N$  è **certamente composto**

se sono entrambi veri  $\Rightarrow N$  è composto con probabilità  $< \frac{1}{4}$ , dunque  $N$  è primo con probabilità  $> \frac{3}{4}$

Iterando il test  $k$  volte, la probabilità di errore diventa  $< (\frac{1}{4})^k$ , con  $k = 30$  diventa inferiore al  $10^{-18}$ . Di seguito l'algoritmo.

```

Verifica(N,y) { //controlla la validita del certificato y (certifica che N sia composto)
    if (P1 == false or P2 == false) return 1; //N certamente composto
    else return 0; //N probabilmente primo (prob errore < 1/4)
}

TestMR(N,k) {
    for (i = 0; i < k; i++) {
        //sceglie a caso y in [2, N-1]
        if (Verifica(N, y) == 1) return 0; //N non primo
    }
    return 1; //N probabilmente primo (prob errore < (1/4)^k)
}

```

**Valutazione di complessità** TestMR costa  $k$  volte Verifica, quindi valuteremo quest'ultimo. Il calcolo dell'MCD, quindi di P1, è facile. Quindi indaghiamo la valutazione di P2: bisognerà calcolare

$y^z \bmod N == 1$  e, in caso non sia verificato

$y^{2^i \cdot z} \bmod N$ , con  $0 \leq i \leq w-1$

Nella seconda parte di P2 v'è calcolato  $y^z \bmod N$ , poi  $y^{2z} \bmod N$  come quadrato del precedente.

L'esponente massimo per  $y$  è  $i = w-1$  (da  $N-1 = 2^w \cdot z$ ), perché  $2^{w-1} \cdot z = \frac{N-1}{2}$

Quindi  $y^{\frac{N-1}{2}} \bmod N$ , al massimo voglio eseguire  $\log N$  moltiplicazioni. La moltiplicazione la sappiamo fare polinomiale, e l'elevamento a potenza possiamo eseguirlo polinomiale con l'**algoritmo delle quadrature successive** o esponenziazione veloce.

$w$  elementi al quadrato con  $w = O(\log N)$ .

Quindi l'algoritmo MR dà un test efficiente per la primalità.

**Algoritmo delle quadrature successive** Vogliamo calcolare  $x = y^z \bmod s$ , con  $x, z, s$  stesso ordine di grandezza.

Si scompone  $z$  in una somma di potenze di 2

$$z = \sum_{i=0}^t k_i \cdot 2^i \text{ con } k_i \in \{0, 1\}$$

Esempio  $z = 45 = 32 + 8 + 4 + 1$

Il massimo  $t$  come visto è  $t = \lfloor \log_2 z \rfloor = \Theta(\log z)$

Si calcolano tutte le potenze  $y^{2^i} \bmod s$  per  $1 \leq i \leq t = \lfloor \log_2 z \rfloor$ , ciascuna come il quadrato della precedente.

$$y^{2^{i+1}} \bmod s = \left( y^{2^i} \right)^2 \bmod s$$

Esempio:  $x = 9^{45} \bmod 11$  e  $45 = 32 + 8 + 4 + 1$ ,  $t = 5$

$$y^2 \bmod s = 9^2 \bmod 11 = 4$$

$$y^4 \bmod s = 4^2 \bmod 11 = 5$$

$$y^8 \bmod s = 5^2 \bmod 11 = 3$$

$$y^{16} \bmod s = 3^2 \bmod 11 = 9$$

$$y^{32} \bmod s = 9^2 \bmod 11 = 4$$

Calcoliamo  $x = y^z \bmod s = \prod_{(i \mid k_i \neq 0)} (y^{2^i}) \bmod s$

Nell'esempio:

$$y^z \bmod s = 9^{45} \bmod 11 = 9^{32+8+4+1} \bmod 11 =$$

$$((9^{32} \bmod 11) \cdot (9^8 \bmod 11) \cdot (9^4 \bmod 11) \cdot (9^1 \bmod 11)) \bmod 11 =$$

$$(4 \cdot 3 \cdot 5 \cdot 9) \bmod 11 = 1$$

**Costo:**  $t = \Theta(\log_2 z)$  quadrature e al più  $t$  moltiplicazioni  $\Rightarrow \Theta(\log_2 z)$  quadrature e  $O(\log z)$  moltiplicazioni. Ogni moltiplicazione ha un costo al più quadratico nel numero di cifre.

Quindi l'algoritmo è **polinomiale nella dimensione dei dati**.

## 2.5.2 Generazione di numeri primi

In pratica è una **generazione di un numero casuale seguita da un test di primalità**. Se il test fallisce, lo si incrementa di due iterando fino a trovare un numero *dichiarato* primo.

Sono pochi i numeri da testare grazie alla densità: il numero di interi primi e minori di  $N$  tendono a  $\frac{N}{\log_e N}$  per  $N \rightarrow \infty$ .

Quindi per  $N$  sufficientemente grande, in un suo intorno di ampiezza  $\log_e N$  cade mediamente un numero primo.

```
Primo(n): { //n: # bit del numero generato
            //genera un numero primo di almeno n bit
            //probabilità errore < (1/4)^k
            S = seq di n-2 bit prodotti da un generatore binario pseudocasuale
            N = (1 S 1) //N ha n bit ed e dispari
            while (TestMR(N,k) == 0) { N = N + 2 } //O(n) = O(log N) volte
            //TestMR costo polinomiale in n = log N -> O(n^3)
            return N;
        }
```

L'algoritmo è polinomiale, circa  $O(n^4)$

## 2.6 Classe RP

**Random Polinomial** Classe dei problemi decisionali verificabili in tempo polinomiale randomizzato.

Dato un problema  $\Pi$ , e  $x$  istanza di input allora  $y$  è un **certificato probabilistico** per l'istanza  $x$  se ha una **lunghezza**  $|y|$  al più polinomiale in  $|x|$  e  $y$  è estratto perfettamente a caso da un insieme associato a  $x$

$A(x, y)$  in tempo polinomiale **attesta con certezza che  $x$  non possiede la proprietà esaminata da  $\Pi$** , cioè  $\Pi(x) = 0$ , oppure **attesta che  $x$  possiede la proprietà esaminata da  $\Pi$  con probabilità  $> \frac{1}{2}$** .





## Capitolo 3

# Cifrari storici

**Scopo** Consentire comunicazioni **sicure** tra poche persone, ma **i cifrari storici sono stati tutti forzati**.

La **cifratura e decifrazione** erano tutte **realizzate a carta e penna**, mentre i **messaggi** da cifrare erano **frasi di senso compiuto** in linguaggio naturale, quindi con l'alfabeto classico di 26 lettere.

### 3.1 Principi di Bacone

XIII Secolo

C e D devono essere **funzioni facili da calcolare**

**Impossibile ricavare D** se C non è nota

Il **crittogramma**  $c = C(m)$  deve **apparire innocente**

### 3.2 Antichi esempi

#### 3.2.1 Scitale

Metodo più antico di cui si ha notizia, inventato dagli spartani nel V secolo a.C.

Asta cilindrica costruita in due esemplari identici posseduti dai due corrispondenti.



#### 3.2.2 Erodoto, Storie

Si tatuava il messaggio sulla testa rasata di un messaggero, si aspettava che ricrescessero i capelli e si portava a destinazione, rivelando il messaggio a seguito di una seconda rasatura.

#### 3.2.3 Enea Tattico

Opera militare del IV secolo a.C. con un capitolo dedicato ai messaggi segreti. Consigliava di inviare un libro qualsiasi sottolineandovi un sottoinsieme di lettere che costituiscono il messaggio, oppure di sostituire le vocali di un testo con altri simboli grafici.

### 3.2.4 Cifrario di Cesare

Il più antico cifrario di concezione moderna. L'idea è che il crittogramma è ottenuto dal messaggio in chiaro sostituendo ogni lettera con quella di 3 posizioni più avanti nell'alfabeto.

Non ha una chiave segreta, e la segretezza dipende dalla conoscenza del metodo: scoprire il metodo significa compromettere irrimediabilmente l'impiego. Il cifrario era quindi destinato all'uso ristretto di un gruppo di conoscenti.

Generalizzandolo a  $k$  posizioni più avanti, si rende più sicuro ( $1 \leq k \leq 25$ ) e si ha  $k$  come chiave segreta.

#### Formulazione matematica

Con  $\text{pos}(X)$  indichiamo la **posizione nell'alfabeto della lettera X**: ad esempio  $\text{pos}(A) = 0$ ,  $\text{pos}(Z) = 25 \dots$ . La chiave  $k$  è quindi  $1 \leq k \leq 25$ , con  $k = 26$  il cifrario lascerebbe invariato il messaggio.

**Cifratura di X** Lettera  $Y$  |  $\text{pos}(Y) = (\text{pos}(X) + k) \bmod 26$

**Decifrazione di Y** Lettera  $X$  |  $\text{pos}(X) = (\text{pos}(Y) - k) \bmod 26$

Un esempio con  $k = 10$ . Cifriamo R, cui  $\text{pos}(R) = 17$ . La sua cifratura è  $(17+10) \bmod 26 = 1 = \text{pos}(B)$ . Quindi  $R \rightarrow B$ .

#### Crittoanalisi

Se si conosce la struttura del cifrario, in breve tempo si possono applicare tutte le chiavi possibili, che sono solo 25, ad un crittogramma: così viene **decifrato** e contemporaneamente si scopre la chiave segreta  $k$ . Come cifrario risulta quindi inutilizzabile a fini crittografici.

**Gode della proprietà commutativa**: data una sequenza di chiavi e di operazioni di cifratura e decifrazione, l'ordine delle operazioni può essere permutato arbitrariamente senza modificare il crittogramma finale.

Per esempio, date  $k_1$  e  $k_2$  chiavi e  $s$  sequenza,

$$C(C(s, k_2), k_1) = C(s, k_1 + k_2)$$

$$D(D(s, k_2), k_1) = D(s, k_1 + k_2)$$

Una sequenza di operazioni di cifratura e decifrazione può essere ridotta ad una sola operazione di cifratura o decifrazione.

Inoltre **comporre più chiavi non aumenta la sicurezza** del sistema.

## 3.3 Classificazione dei cifrari storici

### 3.3.1 Cifrari a sostituzione

Sostituiscono ogni lettera del messaggio in chiaro con una o più lettere dell'alfabeto secondo una regola prefissata.

**Sostituzione monoalfabetica** Es: Cifrario di Cesare.

Alla stessa lettera del messaggio corrisponde sempre una stessa lettera nel crittogramma.

Si possono impiegare funzioni di cifratura e decifrazione più complesse dell'addizione e della sottrazione in modulo, ottenendo uno spazio delle chiavi molto più ampio (ma sempre con una sicurezza molto modesta).

Per esempio, usare come  $k = \langle a, b \rangle$ , cifrare  $\text{pos}(Y) = (a \cdot \text{pos}(X) + b) \bmod 26$  e decifrare

$\text{pos}(X) = a^{-1} \cdot (\text{pos}(Y) - b) \bmod 26$  con  $a^{-1}$  inverso di  $a \bmod 26$  ( $a \cdot a^{-1} = 1 \bmod 26$ ).

C'è quindi un **vincolo forte** sulla chiave:  $\text{MCD}(a, 26) \neq 1 \Rightarrow$  la funzione di cifratura non è iniettiva e la decifrazione diventa impossibile. Ad esempio con  $k = \langle 13, 0 \rangle$  tutte le lettere posizione pari sono trasformate in A, mentre tutte quelle dispari sono trasformate in N.

Le chiavi possibili sono quindi  $12$  (scelte per  $a$ )  $\cdot 26$  (scelte per  $b$ ) =  $312$  chiavi che sono poche.

Se la segretezza dipende unicamente dalla chiave, allora il **numero di chiavi deve essere così grande da essere praticamente immune dal brute force** e deve essere **scelta in modo casuale**.

**Cifrario completo** prendendo una permutazione arbitraria dell'alfabeto come chiave:  
*lettera in chiaro in posizione  $i$   $\rightarrow$  lettera di posizione  $i$  della permutazione.*

La chiave è di 26 lettere, con uno spazio delle chiavi esteso a  $26! - 1$ , cioè circa  $4 \cdot 10^{26}$  chiavi, il che lo rende molto vasto e inesplorabile.

Ma non è comunque sicuro: si può forzare senza ricorrere a brute force, sfruttando la struttura logica dei messaggi in chiaro e l'occorrenza statistica delle lettere.

#### Sostituzione polialfabetica

Alla stessa lettera del messaggio corrisponde una lettera scelta in un insieme di lettere possibili, secondo una regola opportuna (a seconda della posizione o del contesto in cui appare la lettera nel messaggio). L'esempio più antico è l'archivio cifrato di Augusto.

I documenti in archivio erano scritti in numeri, invece che lettere. Augusto li scriveva in greco, poi metteva in corrispondenza la sequenza di lettere del documento con la sequenza di lettere del primo libro dell'Iliade. Sostituiva ogni lettera del documento con il numero che indicava la distanza, nell'alfabeto greco, di tale lettera con quella in pari posizione nell'Iliade.

Per esempio:

Lettera in posizione  $i$  nel documento:  $\alpha$

Lettera in posizione  $i$  nell'Iliade:  $\epsilon$

Carattere in posizione  $i$  nel crittogramma: 4 (distanza tra  $\alpha$  e  $\epsilon$ )

Se la chiave è lunghissima, il cifrario diventa difficile da forzare. Venne usato anche della Seconda Guerra Mondiale, prendendo come chiave una pagina prefissata di un libro e cambiandola di giorno in giorno. Lo **svantaggio** è **registrare per iscritto la chiave**.

**Cifrario di Alberti** con due dischi, dove si cambia chiave ogni volta che si incontra un carattere speciale. Inserendo spesso caratteri speciali (scartati nel messaggio ricostruito) diventa difficile da attaccare e il continuo cambio di chiave rende inutili gli attacchi basati sulla frequenza dei caratteri. La **Macchina Enigma** è un'estensione elettromeccanica del cifrario di Alberti.

**Cifrario di Vigenère**, con una parola segreta  $k$  come chiave. La cifratura di un messaggio  $m$  avviene disponendo  $m$  e  $k$  su due righe adiacenti, allineando le lettere in verticale (se  $k$  è più corta di  $m$  la si ricopia più volte). Ogni lettera  $X$  di  $m$  risulta allineata ad una lettera  $Y$  della chiave. La  $X$  è sostituita nel crittogramma con la lettera che si trova nella cella  $T$  all'incrocio tra la riga che inizia con  $X$  e la colonna che inizia con  $Y$

A	B	C	...	X	Y	Z
B	C	D	...	Y	Z	A
C	D	E	...	Z	A	B
...	...	...	...	...	...	...
X	Y	Z	...	U	V	W
Y	Z	A	...	V	W	X
Z	A	B	...	W	X	Y

Quindi le lettere allineate con A non subiscono modifiche. Quelle allineate con B sono traslate di una posizione in avanti, quelle con R di 17 posizioni...

Una stessa lettera in chiaro è cifrata in modi diversi a seconda della lettera con cui è allineata, mentre per la decifrazione si esegue il processo inverso.

La sicurezza del metodo è influenzata dalla lunghezza della chiave: se contiene  $h$  caratteri, le apparizioni della stessa lettera distanti un multiplo di  $h$  nel messaggio si sovrappongono alla stessa lettera della chiave, quindi sono trasformate nella stessa lettera cifrata.

I cifrari polialfabetici non sono molto più potenti dei monoalfabetici se le chiavi non sono molto lunghe.

Se si estende Vigenère impiegando una chiave lunga quanto il testo, casuale e non riutilizzabile, il cifrario diventa inattaccabile: **one-time pad**.

### 3.3.2 Cifrari a trasposizione

Permutano le lettere del messaggio in chiaro secondo una regola prefissata.

L'idea di base è eliminare qualsiasi struttura linguistica presente nel crittogramma: permutando le lettere del messaggio in chiaro e inserendone eventualmente altre ignorate nella decifrazione.

**Semplice** La chiave è un intero  $h$  e una permutazione  $\pi$  degli interi  $\{1, 2, \dots, h\}$

Nella cifratura si suddivide il messaggio in  $m$  blocchi da  $h$  lettere e si permutano le lettere di ciascun blocco secondo  $\pi$ .

Se la lunghezza di  $m$  non è divisibile per  $h$ , si aggiungono alla fine delle lettere qualsiasi (padding): partecipano alla trasposizione, ma sono ignorate perché la decifrazione le riporta alla fine del messaggio.

Ci sono  $h! - 1$  chiavi ed  $h$  non è fissato a priori: tanto è più grande tanto è più difficile impostare un brute force. Al crescere di  $h$  però cresce anche la difficoltà di ricordare  $\pi$ .

**Permutazione di colonne**  $k = \langle c, r, \pi \rangle$  con:

$c$  ed  $r$  denotano il numero di colonne e righe di una tabella di lavoro  $T$

$\pi$  è una permutazione degli interi  $\{1, 2, \dots, c\}$

Il messaggio  $m$  è decomposto in blocchi  $m_1, m_2 \dots$  di  $c \cdot r$  caratteri.

Nella cifratura i caratteri di ogni blocco sono distribuiti tra le celle di  $T$  in modo regolare, scrivendoli per righe dall'alto verso il basso. Poi le colonne vengono permutate secondo  $\pi$  e si prendono le colonne dalla prima leggendo dall'alto verso il basso e da sinistra verso destra, ottenendo il crittogramma.

**Esempio:**  $\pi = \{2, 1, 5, 3, 4, 6\}$

	1	2	3	4	5	6		2	1	5	3	4	6	
	N	O	N	S	O	N		O	N	O	N	S	N	
	O	I	L	C	O	L		I	O	O	L	C	L	
	P	E	V	O	L	E		E	P	L	V	O	E	
	T							T permutata						
c =	O I E N O P O O L N L V S C O N L E													

Per cifrare il prossimo blocco, si azzerava  $T$  e si ripete il procedimento.

Le chiavi sono teoricamente esponenziali nella lunghezza del messaggio, non essendoci vincoli su  $r$  e  $c$ .

**Cifrario a griglia** Antenato: cifrario di Richelieu. Il crittogramma può essere celato in un libro qualsiasi. La chiave è data da una scheda perforata e dall'indicazione di una pagina del libro: la decifrazione consiste nel sovrapporre la scheda alla pagina, e le lettere visibili attraverso i fori costituiscono il messaggio in chiaro.

## 3.4 Crittoanalisi Statistica

La sicurezza di un cifrario è legata alla dimensione dello spazio delle chiavi. Ci sono altri metodi di attacco: i cifrari storici sono stati violati con un attacco statistico di tipo cipher text.

Nella crittoanalisi statistica si fanno delle ipotesi. Ci sono delle **informazioni note al crittoanalista**: il metodo usare per la cifratura e la decifrazione, il linguaggio naturale con cui è scritto il messaggio e si ammette che il messaggio sia sufficientemente lungo per poter rilevare alcuni dati statistici sui caratteri che compongono il crittogramma.

**Attacco** La frequenza con cui appaiono in media le varie lettere dell'alfabeto è ben studiata in ogni lingua. Dati simili sono noti per le frequenze di diagrammi (gruppi di due lettere consecutive), trigrammi (gruppi di tre lettere) e così via (**q-grammi**).

**Decifrazione cifrari monoalfabetici** Se un crittogramma è generato per sostituzione monoalfabetica allora la frequenza di  $Y$  nel crittogramma è circa la frequenza della corrispondente  $X$  del messaggio.

Nei **cifrari completi** si associano le lettere in base alle frequenze, provando le varie combinazioni. Con le combinazioni di prova, si studiano le frequenze dei possibili diagrammi, dei trigrammi e così via.

**Decifrazione cifrari polialfabetici** Più difficile. Per esempio in Vigenère ogni lettera  $Y$  del crittogramma dipende da una coppia di lettere  $\langle X, K \rangle$  provenienti dal messaggio e dalla chiave.

Se la chiave è di  $h$  caratteri, il crittogramma è composto di  $h$  sottosequenze, ciascuna ottenuta per sostituzione monoalfabetica. Il problema è scoprire  $h$  per scomporre il crittogramma e continuare la decifrazione con il metodo monoalfabetico.

Quindi il messaggio contiene quasi sicuramente gruppi di lettere adiacenti ripetuti più volte. Le apparizioni della stessa sottosequenza allineate con la stessa porzione di chiave danno sottosequenze identiche. Si cercano nel crittogramma coppie di posizioni  $p_1, p_2$  in cui iniziano sottosequenze identiche. La distanza  $d = p_2 - p_1$  è *probabilmente* uguale ad  $h$  o ad un suo multiplo.

**Decifrazione di cifrari a trasposizione** Le lettere nel crittogramma sono le stesse del messaggio in chiaro, non ha senso un attacco statistico basato sulle frequenze: si studiano i  $q$ -grammi

Se si conosce la lunghezza  $h$  della chiave, si divide il crittogramma in porzioni di lunghezza  $h$ , in ciascuna si cercano gruppi di  $q$  lettere che formano i  $q$ -grammi più diffusi. se un gruppo deriva effettivamente da un  $q$ -gramma, si scopre parte della permutazione.

**Conclusione** La rilevazione delle frequenze delle singole lettere del crittogramma è un potente indizio per discernere tra i vari tipi di cifrario:

nei cifrari a trasposizione, l'istogramma delle frequenze coincide circa con quello proprio del linguaggio

nei cifrari a sostituzione monoalfabetica, i due istogrammi coincidono a meno di una permutazione delle lettere

nei cifrari a sostituzione polialfabetica, l'istogramma del crittogramma è assai più appiattito di quello del linguaggio



## Capitolo 4

# Cifrari perfetti

Shannon, 1949

**Cifrario perfetto** Sono cifrari che ci offrono una **sicurezza incondizionata**, proteggono le informazioni con certezza assoluta indipendentemente dalla potenza di calcolo. Si rende **essenziale avere la chiave**, un'attacco **brute force non permette di decifrare**.

Informalmente, un cifrario è perfetto se la **sicurezza è garantita qualunque sia l'informazione carpita dal canale di comunicazione**.

Abbiamo quindi due spazi:

MSG: lo **spazio dei messaggi**

CRITTO: lo **spazio dei crittogrammi**

e due variabili aleatorie:

M: descrive il **comportamento del mittente**, con valori in MSG

C: descrive il **processo di comunicazione**, con valori in CRITTO

Ho delle probabilità:

$P(M = m)$ : probabilità che il mittente voglia spedire il messaggio  $m$

$P(M = m \mid C = c)$ : probabilità condizionata che il messaggio inviato sia  $m$  posto che sul canale stia transitando il crittogramma  $c$

Con  $\forall m \in \text{MSG}$  e  $\forall c \in \text{CRITTO}$ .

Scenario: il crittoanalista conosce tutto del sistema tranne la chiave, quindi conosce:

la distribuzione di probabilità con cui il mittente invia i messaggi

cifrario utilizzato

lo spazio delle chiavi (KEY)

**Definizione** Un cifrario è perfetto se  $\forall m \in \text{MSG}$  e  $\forall c \in \text{CRITTO}$ , allora  $P(M = m) = P(M = m \mid C = c)$ , cioè la conoscenza di  $c$  non raffina la conoscenza. In un cifrario perfetto, la conoscenza del crittoanalista non cambia dopo che è stato osservato un crittogramma in transito. Quindi **il messaggio ed il crittogramma appaiono del tutto scorrelati, nessuna informazione sul messaggio filtra dal crittogramma**.

### 4.0.1 Teorema di Shannon

In un cifrario perfetto il numero delle chiavi deve essere maggiore o uguale del numero dei messaggi possibili (cioè con probabilità non nulla di essere inviati)

**Dim** Per assurdo

$N_m = \#$  dei messaggi possibili, cioè  $m \in \text{MSG} \mid P(M = m) > 0$

$N_k = \#$  delle chiavi

Suppongo per assurdo che  $N_k < N_m$ . Suppongo  $c \in \text{CRITTO}$  con  $P(C = c) > 0$ . Conto i messaggi che possono corrispondere al crittogramma  $\Rightarrow s$  messaggi potenzialmente corrispondenti a  $c$ . Questi  $s$  messaggi sono i messaggi che posso ottenere decifrando  $c$  con ogni chiave possibile: con la chiave  $k_1$  ottengo  $m_1$ ,  $k_2$  ottengo  $m_2$ , ma anche possibile che con  $k_3$  ottenga di nuovo  $m_2$  dato che non so come funziona il cifrario. Posso dire con certezza che  $s \leq N_k$  e per ipotesi  $N_k < N_m$

Ottingo  $s < N_m \Rightarrow \exists m \in \text{MSG}$  con  $P(M = m) > 0 \mid P(M = m \mid C = c) = 0$ , ottenendo una conoscenza maggiore (posso escludere  $m$ ) quindi il cifrario non è perfetto, ottenendo una **contraddizione**.

#### 4.0.2 One-Time Pad

1917, Mauborgne, Vernam

Usa l'alfabeto binario  $\{0,1\}$ , usato sia durante le guerre mondiali che durante la guerra fredda. L'idea è avere una chiave lunghissima consumata man mano e mai riutilizzata.

MSG, CRITTO e KEY sono spazi di sequenze binarie. La regola è pubblica e usa lo xor. Quindi sia C che D usano lo xor (somma in modulo 2) per trasformare il messaggio nel crittogramma e viceversa.

$m \in \{0,1\}^n$  e  $k \in \{0,1\}^n$  con  $n > 0$  fissato.

$c = C(m, k) = m \oplus k$  Con  $n = 5$ ,  $m = 10110$ ,  $k = 01011$  allora  $c = 11101$ .

La decifrazione  $m = D(c, k) = c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m$  perché  $k \oplus k = 0 \dots 0$

**Fondamentale non riutilizzare la chiave.** Questo perché avendo  $c', c''$  ottenuti con la stessa  $k$  da  $m', m''$ , faccio  $c' \oplus c'' = (m' \oplus k) \oplus (m'' \oplus k) = m' \oplus m'' \oplus (k \oplus k) = m' \oplus m''$ , acquisendo conoscenza (lungi tratti di 0 significa tratti uguali nei messaggi in chiaro).

**Teorema** Quando il One-Time Pad è perfetto. Ipotesi:

1. Tutti i messaggi hanno lunghezza  $n$ , con del padding o divisione in blocchi all'occorrenza
2. Tutte le sequenze di  $n$  bit sono messaggi possibili (per quelle prive di senso probabilità molto bassa ma comunque  $> 0$ )
3. Chiave scelta **perfettamente a caso per ogni messaggio**

Il **teorema** dice che sotto 1, 2 e 3 One-Time Pad è **un cifrario perfetto e minimale** (usa un numero minimo di chiavi)

**Dim** Dimostro che è perfetto, cioè che  $\forall m \in \text{MSG}$  e  $\forall c \in \text{CRITTO}$ , allora  $P(M = m) = P(M = m \mid C = c)$   
 $P(M = m \mid C = c) = \frac{P(M=m \wedge C=c)}{P(C=c)} = \frac{P(M=m) \cdot P(C=c)}{P(C=c)} = P(M = m)$

Per le proprietà dello xor, fissato  $m$  chiavi diverse producono crittogrammi diversi  $\Rightarrow \exists!$  chiave  $k \mid m \oplus k = c \forall c \in \text{CRITTO}$ ,  $P(C = c) = P(\text{scegliere l'unica chiave } k \mid m \oplus k = c) = \frac{1}{2^n}$ , questo perché  $\{M = m\}$  e  $\{C = c\}$  sono **eventi indipendenti**.

Per quanto riguarda la minimalità, cioè  $N_k \geq N_m$ , il One-Time Pad per ogni  $n$  ha  $N_k = N_m = N_{\text{CRITTO}} = 2^n$ , questo perché anche le chiavi sono sequenze di  $n$  bit come i messaggi e i crittogrammi.

#### Attacchi

Bruteforce: non ha senso, ogni chiave fa ricostruire un messaggio possibile quindi non aggiunge conoscenza

Rimane il problema di generare le sequenze di bit completamente casuali.

**Osservazione** Rimuoviamo la seconda ipotesi nella dimostrazione. Per esempio in inglese i messaggi significativi sono circa  $\alpha^n \ll 2^n$  con  $\alpha = 1.1$

Quindi  $N_m = \alpha^n$ ,  $N_k \geq N_m$  cioè  $N_k \geq \alpha^n$ , la chiave sarà una sequenza di  $t$  bit con  $t \mid 2^t \geq \alpha^n$

Risolvero trovando  $t \geq \log_w \alpha^n = n \log_2 \alpha = 0.12 \cdot n$

Per confondere l'avversario è opportuno che coppie diverse  $(m, k)$  producano lo stesso crittogramma  $\Rightarrow \#$  coppie  $(m, k) \gg \#$  crittogrammi, cioè  $\alpha^n 2^t \gg 2^n$



## 4.1 Principi di Shannon

Principi per la resistenza agli attacchi di crittoanalisi statistica:

**Diffusione:** tutti i caratteri del testo in chiaro si devono spargere nel crittogramma.

**Confusione:** combinare testo in chiaro e chiave in modo complesso, per non permettere al crittoanalista di sapere le due sequenze analizzando il crittogramma.

**Standard** 1972 NBS (National Bureau of Standards) → 1973 NIST (National Institute for Security and Technology)

**Sicurezza basata sulla segretezza della chiave** e non sul processo di cifratura e decifrazione (che è **pubblico**)

**Algoritmo efficiente** in software e hardware

IBM propone **LUCIFER**, poi migliorato con l'NSA. Da 128 bit a 56 bit per la chiave: variazioni nella s-box.

Si arriva al 1977 con il **DES**, accettato e reso pubblicamente disponibile (licenza d'uso gratuita): **Data Encryption Standard**. Rimane fino al 1999, quando si sconsiglia il DES in favore del 3DES. Dal 2005 anche il 3DES risulta superato, al suo posto **AES (Advanced Encryption Standard)**

## 4.2 Data Encryption Standard

Cifratura a blocchi di 64 bit e chiave segreta di 64 bit: 56 bit casuali e 8 bit di parità suddivisi in: 7 bit, bit parità, 7 bit, bit parità...

$r = 16$  fasi in cui si ripetono le stesse operazioni.



### Struttura del DES

$m$ : blocco del messaggio

$c$ : corrispondente blocco del crittogramma

$k$ : chiave segreta con i bit di parità

$\forall i = 1, \dots, 16$  ho

$$S[i] = D[i - 1]$$

$$D[i] = S[i - 1] \oplus f(D[i - 1], k[i - 1])$$

$f$ : funzione **non** lineare

Fase  $i$ -esima del DES

## Permutazioni

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutazione PI

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Permutazione PF

57	49	41	33	25	17	9	
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	
7	52	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

Trasposizione T

Le tabelle vanno lette per righe.

**Permutazione PI:** riordina i bit del messaggio  $m = m_1 m_2 \dots m_{64}$  come  $m_{58} m_{50} \dots m_7$ : ad esempio porta in posizione 40 (numero della cella) il bit in posizione 1 (contenuto della cella)

**Permutazione PF:** è l'inversa di PI, cioè nell'esempio riporta in posizione 1 il bit in posizione 40

**Trasposizione T:** provvede anche a scartare dalla chiave  $k = k_1 k_2 \dots k_{64}$  i bit di controllo  $k_8, k_{16}, \dots, k_{64}$ , generando una sequenza di 56 bit che costituisce la prima sottochiave  $k[0]$

## Funzioni CT e EP

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Funzione CT

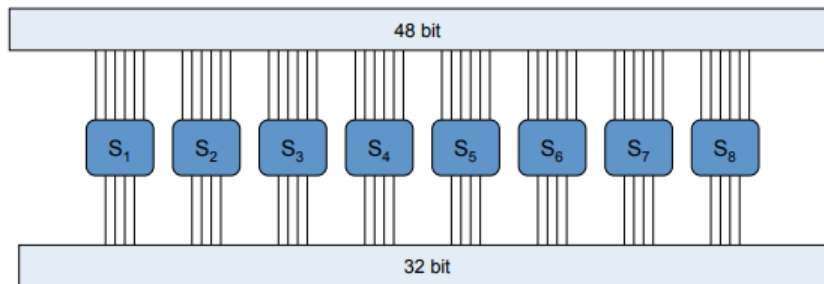
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Funzione EP

**Funzione CT:** 8 bit dell'ingresso (es: il bit 9) non sono presenti in uscita

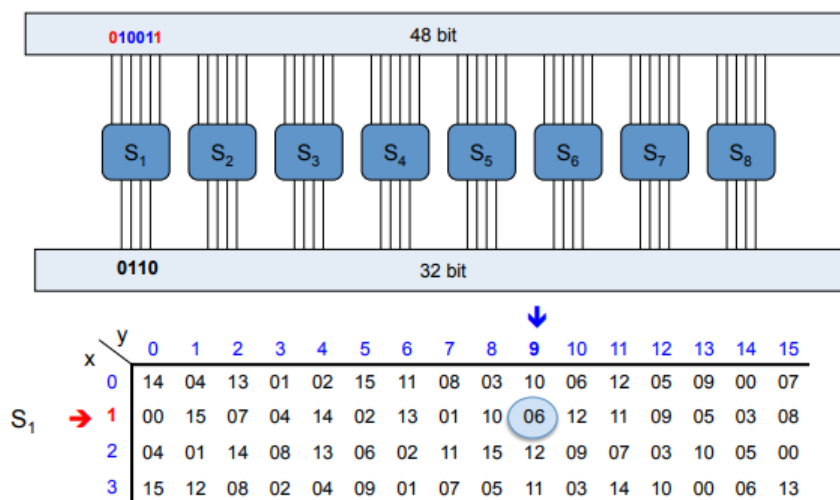
**Funzione EP:** 16 bit di ingresso sono duplicati (es: il bit 32 è copiato nelle posizioni 1 e 47 dell'uscita)

## S-box



x \ y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Tabella che definisce la sottofunzione  $S_1$ . Le sottofunzioni  $S_2, \dots, S_8$  sono definite in modo simile.



**Permutazione P**

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Permutazione di 32 bit che genera il blocco finale  $D[i]$ .

**Attacchi** Due metodi principali:

1. Architetture apposite progettate per attaccare il DES
2. Calcolo distribuito su più macchine

**Attacchi esaurienti Chosen Plain Text:** il crittoanalista si procura coppie  $\langle m, c_1 \rangle, \langle \bar{m}, c_2 \rangle$

Da  $C(m, k) = \begin{cases} c_1 \Rightarrow k \text{ probabile chiave} \\ c_2 \Rightarrow \bar{k} \text{ probabile chiave} \end{cases}$

**Crittoanalisi differenziale**  $2^{47}$  coppie  $\langle m, c \rangle$  scelti dal crittoanalista. L'attacco costa complessivamente  $2^{55}$  con  $r = 16$ .

**4.2.1 Varianti del DES**

**Scelta indipendente delle sottochiavi di fase**  $\# \text{ bit } 56 \rightarrow 16 \cdot 48 = 768 \text{ bit}$   
 Crittoanalisi differenziale  $\rightarrow 2^{61}$

**Cifatura multipla**  $\forall k_1, k_2$  ho  $C_D(C_D(n, k_1), k_2) \neq C_D(n, k_3)$ , questo  $\forall n, k_3$   
 $\#$  spazio delle chiavi =  $2^{112}$ , non sono 112 bit di sicurezza  
 Sicurezza pari a quella di una chiave da 57 bit

**Attacco "Meet in the Middle"**  $c = C(C(n, k_1), k_2)$ , con  $k_1, k_2$  chiavi di 56 bit  $\rightarrow D(c, k_2) = C(n, k_1)$   
 Si prende una coppia  $\langle n, c \rangle$

$\forall k_1$  calcolo e salvo  $C(n, k_1)$  ( $2^{56}$ )

$\forall k_2$  calcolo  $D(c, k_2)$  e lo cerco nella lista delle cifrature

Deve **esistere certamente almeno una corrispondenza** ( $N = 2^{56}$ )

$N = 2^{56}$  cifrature +  $O(N)$  decifrazioni

Quindi costo  $2N \ll N^2$  (costo dell'enumerazione di tutte le coppie  $(k_1, k_2)$ )

**3DES** TDEA = Triple Data Encryption Algorithm

2TDEA, 3TDEA: 2 e 3 sono  $\#$  chiavi

**2TDEA**

$c = C(D(C(n, k_1), k_2), k_1)$ , con  $k_1, k_2$  chiavi di 56 bit tra loro indipendenti.

$k_1 = k_2 \Rightarrow$  2TDEA equivale ad una singola cifratura DES. CDC non è più robusto di CCC, 112 bit di sicurezza.

**3TDEA**

$c = C(D(C(n, k_1), k_2), k_3)$ , con  $k_1, k_2, k_3$  chiavi di 56 bit tra loro indipendenti.

$\#$  bit della chiave:  $56 \cdot 3 = 168 \text{ bit}$

Vulnerabile a meet in the middle  $\rightarrow$  112 bit di sicurezza

$$m = D(C(D(c, k_3), k_2)k_1) \Rightarrow C(m, k_1) = C(D(c, k_3), k_2)$$

1. Enumero le chiavi di 56 bit e salvo la lista  $C(m, k_1) \forall k_1 \in \{0, 1\}^{56}$
2.  $\forall k_2, k_3$  calcolo  $C(D(c, k_3), k_2)$  e lo cerco nella lista  
 $2^{56} + 2^{112}$ ,  $2^{56}$  dal punto 1 e  $2^{112}$  costo di enumerazione delle coppie  $k_2, k_3$

**AES** 128 bit di chiave

Ogni sottochiave di fase,  $w(i)$ , è una sequenza di 4 byte che usa la s-box.

$$k = \begin{array}{|c|c|c|c|} \hline & & & \text{1byte} \\ \hline & & & \\ \hline & & & \\ \hline & & & \\ \hline \end{array}$$

$w(0) \quad w(1) \quad w(2) \quad w(3)$

Chiave:  $w(0), w(1), w(2), w(3)$

$$\forall t \geq 4 \text{ ho } w(t) = \begin{cases} w(t-1) \oplus w(t-4) & \text{se } 4 \nmid t \\ T(w(t-1)) \oplus w(t-4) & \text{se } 4 \mid t \end{cases} \quad \text{con } T \text{ non lineare e che usa la s-box}$$

Chiave alla  $i$ -esima fase,  $1 \leq i \leq 10$ :  $w(4i), w(4i+1), w(4i+2), w(4i+3)$

**Cifratura** Blocchi di 128 bit, riempita per colonne  $b_{ij} \in \{0, 1\}^8$

$$B = \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}$$

Trasformazione iniziale:  $k$  matrice della chiave, con  $B$  costruisco  $B \oplus k$   
 10 fasi da 4 operazioni:

#### 01 SUBSTITUTE BYTES

Ogni byte di  $B$  è trasformato usando s-box:  $b_{ij} \rightarrow \text{s-box}(b_{ij})$

#### 02 SHIFT ROWS

#### 03 MIX COLUMNS, non si applica nella fase 10

#### 04 ADD ROUND KEY

Alla fine delle 10 fasi, il blocco  $B$  è il crittogramma

**S-box** Matrice  $16 \times 16$  di interi  $\in (0, 255) \Rightarrow$  contiene una permutazione

$$b_{ij} \rightarrow \text{s-box}(b_{ij}) \in \{0, 1\}^8$$

$$b_{ij} = b_1 b_2 b_3 b_4 | b_5 b_6 b_7 b_8$$

Riga:  $b_1 b_2 b_3 b_4, 0 \leq x \leq 15$

Colonna:  $b_5 b_6 b_7 b_8, 0 \leq y \leq 15$

$$\text{Es } b_{ij} = 1000|1011 = 8|11, \text{ s-box}[8, 11] \rightarrow 61 \text{ cioè } 00111101$$

$x \text{ byte} \xrightarrow{\text{s-box}} x^{-1}$  inverso moltiplicativo + composizione lineare in  $\text{GF}(2^8)$

Galois Field, campi finiti di Galois

#### 02 SHIFT ROWS

$$\begin{array}{cccc} \underline{b_{00}} & b_{01} & b_{02} & b_{03} \\ \underline{b_{10}} & b_{11} & b_{12} & b_{13} \\ \underline{b_{20}} & b_{21} & b_{22} & b_{23} \\ \underline{b_{30}} & b_{31} & b_{32} & b_{33} \end{array} \rightarrow \begin{array}{cccc} \underline{b_{00}} & b_{01} & b_{02} & b_{03} \\ \underline{b_{11}} & b_{12} & b_{13} & \underline{b_{10}} \\ \underline{b_{22}} & b_{23} & \underline{b_{20}} & \underline{b_{21}} \\ \underline{b_{33}} & \underline{b_{30}} & \underline{b_{31}} & b_{32} \end{array}$$

#### 03 MIX COLUMNS

$M$  matrice di  $4 \times 4$  byte. Ogni colonna del blocco  $B$   $B_j \rightarrow M \cdot B_j$ , con  $0 \leq j \leq 3$

Il nuovo  $b_{ij}$  diventa un valore che dipende da tutti i byte della colonna  $(b_{0j}, b_{1j}, b_{2j}, b_{3j})$

$$b_{ij} \rightarrow b_{ij} \oplus k_{ij}$$



## Capitolo 5

# Crittografia a Chiave Pubblica

Cifrari ibridi, usati per lo **scambio delle chiavi**.

### One-Time Pad 1917

Non può essere decifrato senza conoscere la chiave. **Assolutamente sicuro**, ma richiede una nuova chiave segreta per ogni messaggio, che deve essere perfettamente casuale e lunga quanto il messaggio da scambiare. Diventa molto attraente per chi richiede una sicurezza assoluta ed è disposto a pagarne i costi.

Ma **come si genera e come si scambia la chiave?**

## 5.1 AES

**Advanced Encryption System** Standard per le comunicazioni riservate ma non-classificate. Pubblicamente noto e realizzabile su hardware di ogni tipo, con chiavi brevi (128/256 bit, qualche decina di caratteri)

Ma come scambiare in sicurezza una chiave segreta? La chiave serve per comunicare in sicurezza, ma deve essere stabilita comunicando *in sicurezza* senza poter ancora usare il cifrario.

### 5.1.1 Protocollo DH

Nel 1976 viene proposto un algoritmo per generare e scambiare una chiave segreta su un canale insicuro, senza necessità che le due parti si siano scambiate informazioni o incontrate in precedenza. Il **protocollo DH** è un algoritmo ancora usato nei protocolli crittografici su Internet. Diffie e Hellman propongono anche la definizione di crittografia a chiave pubblica, ma senza avere un'implementazione pratica.

### 5.1.2 Cifrari simmetrici

Nei **cifrari simmetrici**, la **chiave di cifratura è uguale a quella di decifrazione** (o l'una può essere facilmente calcolata dall'altra) ed è **nota solo ai due partner** che la scelgono di comune accordo e la mantengono **segreta**.

### 5.1.3 Cifrari asimmetrici

Nei **cifrari a chiave pubblica** l'obiettivo è **permettere a tutti di inviare messaggi cifrati ma abilitare solo il ricevente (Bob) a decifrarli**.

Le **operazioni di cifratura e decifrazione sono pubbliche** e usano **due chiavi diverse**:

$k_{pub}$  per **cifrare: pubblica**

$k_{priv}$  per **decifrare: privata**, nota solo a Bob

Esiste una coppia  $\langle k_{pub}, k_{priv} \rangle$  per ogni utente del sistema, scelta da questi nella sua veste di possibile destinatario.

**Cifratura** La **cifratura di un messaggio da spedire** a Bob è eseguita da qualunque mittente come

$$c = C(m, k_{pub})$$

La chiave  $k_{pub}$  e la funzione di cifratura  $C(m, k)$  sono note a tutti.

**Decifrazione** La decifrazione di un messaggio ricevuto da Bob è eseguita da Bob come

$$m = D(c, k_{priv})$$

La funzione di decifrazione  $D(c, k)$  è nota a tutti **ma la chiave  $k_{priv}$  non è disponibile agli altri.**

**Ruoli** Ruoli completamente diversi svolti da mittente e destinatario di un messaggio, che hanno invece ruoli intercambiabili nei cifrari simmetrici dove condividono la solita informazione (chiave segreta)

### Tre elementi

#### 1. Correttezza del processo di cifratura e decifrazione

Bob deve interpretare qualunque messaggio che gli altri utenti decidano di spedirgli. Quindi **per ogni possibile messaggio  $m \Rightarrow D(C(m, k_{pub}), k_{priv}) = m$**

#### 2. Efficienza e sicurezza del sistema

##### Generazione casuale delle chiavi

La **coppia di chiavi è facile da generare** e deve risultare praticamente impossibile che due utenti scelgano la stessa chiave.

##### Adottabilità del sistema

Dati  $m$  e  $k_{pub}$ , è **facile per Alice calcolare il crittogramma  $c = C(m, k_{pub})$**

Dati  $c$  e  $k_{priv}$ , è **facile per Bob calcolare il messaggio  $m = D(c, k_{priv})$**

#### 3. Sicurezza del cifrario

Pur conoscendo il crittogramma  $c$ , la chiave pubblica e le funzioni  $C$  e  $D$ , è **difficile per il crittoanalista risalire al messaggio  $m$**

**Cifratura** La funzione  $C$  deve essere una **one-way trapdoor**: calcolare  $c = C(m, k_{pub})$  deve essere **computazionalmente facile**, ma **decifrare  $c$  computazionalmente difficile**. Questo a meno di un **meccanismo segreto (trapdoor)** rappresentato da  $k_{priv}$

## 5.2 RSA

**Rivest, Shamir, Adleman** Proposto come un sistema a chiave pubblica basato su una funzione *facile* da calcolare e *difficile* da invertire: la moltiplicazione di due primi  $p$  e  $q$ .

Calcolare  $n = p \cdot q$  è **facile**

Calcolare  $p, q$  da  $n$  è **difficile, a meno di non conoscere uno dei due fattori.**

Fa uso dell'**algebra modulare**:

Riduce lo spazio dei numeri su cui si opera, e quindi aumenta la velocità di calcolo

Rende **difficili** problemi computazionali che risultano facili o banali nell'algebra non modulare.

Le funzioni tendono a comportarsi in modo imprevedibile.

**Funzione di Eulero** Numero di interi minori di  $n$  e coprimi con esso

$$\phi(n) = |Z_n^*|$$

$n$  primo  $\Rightarrow \phi(n) = n - 1$

$Z_n = \{0, 1, 2, \dots, n-1\}$ , e  $Z_n^* \subseteq Z_n$  è l'insieme degli elementi di  $Z_n$  coprimi con  $n$ . Se  $n$  è primo allora

$Z_n^* = \{1, 2, \dots, n-1\}$ . Se non è primo, calcolare  $Z_n^*$  è computazionalmente difficile (direttamente proporzionale al valore di  $n$ ).

**Teorema**  $n$  composto  $\Rightarrow \phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_k})$  con  $p_1, \dots, p_k$  fattori primi di  $n$  senza molteplicità.

**Teorema**  $n$  semiprimo (prodotto di due primi), cioè  $n = p \cdot q \Rightarrow \phi(n) = (p-1) \cdot (q-1)$

**Teorema di Eulero** Per  $n > 1$  e  $\forall a$  primo con  $n$  si ha  $a^{\phi(n)} \equiv 1 \pmod{n}$

**Piccolo teorema di Fermat** Per  $n$  primo e  $\forall a \in Z_*$  si ha  $a^{n-1} \equiv 1 \pmod{n}$



Come conseguenze si ha che per qualunque  $a$  primo con  $n$   $a \cdot a^{\phi(n)-1} \equiv 1 \pmod n$  e  $a \cdot a^{-1} \equiv 1 \pmod n$  e quindi

$$a^{-1} \equiv a^{\phi(n)-1} \pmod n$$

L'inverso  $a^{-1}$  di  $a \pmod n$  si può calcolare per esponenziazione di  $a$  se si conosce  $\phi(n)$ . In generale, nell'algebra modulare **l'esistenza dell'inverso non è garantita** perché  $a^{-1}$  deve essere intero.

$ax \equiv b \pmod n$  ammette soluzione  $\Leftrightarrow \text{MCD}(a, n) \mid b$  con  $\text{MCD}(a, n)$  soluzioni distinte.

Quindi  $ax \equiv b \pmod n$  ammette **unica soluzione**  $\Leftrightarrow \text{MCD}(a, n) = 1 \Leftrightarrow \exists a^{-1}$  inverso di  $a$

$ax \equiv 1 \pmod n$  ammette esattamente una soluzione ( $a^{-1}$ )  $\Leftrightarrow a, n$  primi fra loro.

### 5.2.1 Generatori

$a \in Z_n^*$  è un **generatore** di  $Z_n^*$  se la funzione  $a^k \pmod n$  con  $1 \leq k \leq \phi(n)$  **genera tutti e soli gli elementi** di  $Z_n^*$ . Produce come risultati tutti gli elementi di  $Z_n^*$  ma in un ordine difficile da prevedere.

**Teorema di Eulero**  $a^{\phi(n)} \pmod n = 1 \Rightarrow 1 \in Z_n^*$  è un generatore per  $k = \phi(n)$

Per ogni generatore  $a^k \not\equiv 1 \pmod n$

**Esempio** 3 genera  $Z_7^*$

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$ ,  $\phi(7) = 6$

$3^k \pmod 7 = 3, 2, 6, 4, 5, 1$  con  $1 \leq k \leq 6 = \phi(7)$

Esistono valori di  $n$  per cui  $Z_n^*$  non ha generatori. Ad esempio,  $Z_8^*$  non ammette generatori.

**Teorema:** se  $n$  è primo  $\Rightarrow Z_n^*$  ha almeno un generatore.

Per  $n$  primo, non tutti gli elementi di  $Z_n^*$  sono suoi generatori. Ad esempio 1 non è mai generatore, e altri elementi possono non essere generatori. Per  $n$  primo sappiamo che i generatori di  $Z_n^*$  sono in totale  $\phi(n-1)$

### Problemi sui generatori rilevanti in crittografia

**Determinare un generatori di  $Z_n^*$  con  $n$  primo** Si possono provare tutti gli interi in  $[2, n-1]$  fino a trovare il generatore: tempo **esponenziale** nella dimensione di  $n$ . Il problema è computazionalmente difficile, risolto con **algoritmi randomizzati**, con alta probabilità di successo.

**Calcolo del logaritmo discreto** Risolvere in  $x$  l'equazione  $a^x \equiv b \pmod n$  con  $n$  primo.

Ammette una soluzione per ogni valore di  $b \Leftrightarrow a$  è un generatore di  $Z_n^*$ . Tuttavia:

non è noto a priori in che ordine sono generati gli elementi di  $Z_n^*$

quindi non è noto per quale valore di  $x$  si genera  $b \pmod n$

un esame diretto della successione richiede tempo esponenziale nella dimensione di  $n$

non è noto un algoritmo polinomiale di soluzione

### Funzioni One-Way Trapdoor

Esistono funzioni matematiche che sembrano possedere i requisiti richiesti (proprietà di teoria dei numeri e di algebra modulare). Il loro calcolo risulta **incondizionatamente semplice** e la loro **inversione è semplice se si dispone di un'informazione aggiuntiva sui dati** (chiave privata). Senza questa informazione, l'inversione richiede la soluzione di un problema NP-hard, o comunque di un problema noto per cui non si conosce un algoritmo polinomiale.

Alcuni esempi:

**Fattorizzazione**  $n = p \cdot q$  è facile, tempo quadratico nella lunghezza della rappresentazione.

Invertire, cioè ricostruire  $p$  e  $q$  da  $n$  richiede tempo esponenziale (per quanto noto fin'ora, anche se non vi è dimostrazione che sia NP-hard. L'esistenza di un algoritmo polinomiale è improbabile ma non da escludere)

**Trapdoor:** se si conosce  $p$  o  $q$ , la chiave segreta, ricostruire l'altro è facile.

**Calcolo della radice in modulo** Calcolare  $y = x^z \pmod s$  con  $x, z, s$  interi richiede tempo polinomiale ( $\Theta(\log_2 z)$  moltiplicazioni con esponenziazioni successive)

Se  $s$  non è primo, invertire e calcolare  $x = y^{\frac{1}{z}} \pmod s$  richiede tempo esponenziale per quanto noto.

Se  $x$  è primo con  $s$  e si conosce  $v = z^{-1} \pmod \phi(s)$  (chiave segreta),  $x$  si può facilmente determinare con  $x = y^v \pmod s$  per il teorema di Eulero.

**Calcolo del logaritmo discreto** Calcolare  $y = x^z \bmod s$  è facile, ma invertire rispetto a  $z$  cioè calcolare  $z$  tale che  $y = x^z \bmod s$  dati  $x, y, s$  è difficile.

Gli algoritmi noti hanno la stessa complessità della fattorizzazione, quindi si può introdurre una trapdoor.

## 5.2.2 Crittografia a chiave pubblica

### Vantaggi

Se gli utenti di un sistema sono  $n$ , il numero complessivo di chiavi (pubbliche e private) è  $2n$  invece di  $n(n-1)/2$

Non è richiesto alcuno scambio segreto di chiavi

### Svantaggi

Sono sistemi molto più lenti dei cifrari simmetrici

Sono esposti ad attacchi chosen plain-text

## 5.2.3 Cifrari ibridi

Si usa un cifrario a chiave segreta (AES) per le comunicazioni di massa

e un cifrario a chiave pubblica per scambiare le chiavi segrete relative al primo, senza incontri fisici tra gli utenti

La trasmissione dei messaggi lunghi avviene ad alta velocità, mentre è lento lo scambio delle chiavi

Le chiavi sono composte al massimo da qualche decina di byte

L'attacco chosen plain-text è risolto se l'informazione cifrata con la chiave pubblica (chiave segreta dell'AES) è scelta in modo da risultare imprevedibile al crittoanalista

La chiave pubblica deve essere estratta da un certificato digitale valido, per evitare attacchi man-in-the-middle (MITM)

## 5.2.4 RSA

Il cifrario è diviso in varie fasi.

**Creazione della coppia di chiavi** Il destinatario ha l'onere di creare le chiavi:

DEST sceglie  $p$  e  $q$  primi **molto grandi** (migliaia di bit):  $n = p \cdot q$  deve avere 2048 bit, ancora più a lungo termine 3072 bit.

Si esegue in tempo polinomiale, primalità via Miller-Rabin

DEST calcola  $n = p \cdot q$ ,  $\phi(n) = (p-1) \cdot (q-1)$

Anche questo in tempo polinomiale

DEST sceglie  $e < \phi(n) \mid \text{MCD}(e, \phi(n)) = 1$  (coprimo con  $\phi(n)$ )

Polinomiale

DEST calcola  $d = e^{-1} \bmod \phi(n)$

$\exists!$  perché  $e$  è coprimo con  $\phi(n)$

Polinomiale con algoritmo di Euclide esteso

DEST rende pubblica  $k[\text{pub}] = \langle e, n \rangle$  **chiave pubblica**

Tiene private  $k[\text{priv}] = \langle d \rangle$  **chiave privata**

**Messaggio** Sequenza binaria trattata come un intero  $m < n$ . Se  $m \geq n$ ,  $m$  si divide in blocchi di  $b = \lfloor \log_2 n \rfloor$  bit, cifrati indipendentemente, sennò ci sarebbero collisioni in fase di decifratura.

Nella pratica si fissa un limite inferiore comune per la dimensione dei blocchi  $b \mid m < 2^b < n$

**Cifratura** Mittente si occupa di costruire  $c = C(m, k[\text{pub}]) = m^e \bmod n \Rightarrow c < n$

Polinomiale via quadrature successive

**Decifrazione** Destinatario è l'unico che può ricavare  $m = D(c, k[\text{priv}]) = c^d \bmod n$

Polinomiale via quadrature successive

**Esempio**  $p = 5, q = 11 \Rightarrow n = 55, \phi(n) = (p-1)(q-1) = 40$   
 $e = 7, \text{MCD}(7, 40) = 1$  ok  
 $d = 7^{-1} \bmod 40 = -17 \bmod 40 = 23 \bmod 40 = 23$

$$\text{EE}(7, 40) \uparrow \langle 1, -17 \rangle$$

$$\text{EE}(40, 7) \uparrow \langle 1, 3, -17 \rangle$$

$$\text{EE}(7, 5) \uparrow \langle 1, -2, +3 \rangle$$

$$\text{EE}(5, 2) \uparrow \langle 1, 1, 0 - \lfloor 5/2 \rfloor \cdot 1 \rangle = \langle 1, 1, -2 \rangle$$

$$\text{EE}(2, 1) \uparrow \langle 1, 0, 1 - \lceil 2/1 \rceil \cdot 0 \rangle = \langle 1, 0, 1 \rangle$$

$$\text{EE}(1, 0) \rightarrow \langle 1, 1, 0 \rangle$$

**Correttezza** Dim che  $D(C(m, k[\text{pub}]), k[\text{priv}]) = m$

$$c^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m$$

**Teorema**  $\forall m < n$  si ha  $m^{ed} \bmod n = m$ , **dimostro** per casi:

1.  $p, q$  non dividono  $m$   
 $\Rightarrow \text{MCD}(m, n) = 1$ , sono coprimi  
 $\Rightarrow m^{\phi(n)} \equiv 1 \bmod n$  (th. Eulero)  
 $\Rightarrow e \cdot d \equiv 1 \bmod \phi(n)$ , quindi  $e \cdot d = 1 + r \cdot \phi(n)$  con  $r \in \mathbb{N}$  (def. di inverso)  
 $\Rightarrow m^{ed} \bmod n = m^{1+r\phi(n)} \bmod n = m \cdot (m^{\phi(n)})^r \bmod n = m \cdot 1^r \bmod n = m \bmod n = m$  perché  $m < n$  ok
2.  $m, n$  non sono coprimi, suppongo  $p \mid m$  e  $q \nmid m$  (analogo invertendo  $p$  e  $q$ )  
 $\Rightarrow p \mid m \Rightarrow m \equiv 0 \bmod p$   
 $\Rightarrow \forall r \in \mathbb{N}$  ho  $m^r \equiv 0 \bmod p$   
 $\Rightarrow \forall r \in \mathbb{N}$  ho  $m^r - m \equiv 0 \bmod p$   
 $\Rightarrow$  con  $r = e \cdot d$  ho  $m^{ed} - m \equiv 0 \bmod p$   
 $\Rightarrow \text{MCD}(q, m) = 1$  sono coprimi  
 $\Rightarrow m^{\phi(q)} \equiv 1 \bmod q$   
 $\Rightarrow m^{ed} \bmod q = m^{1+r\phi(n)} \bmod q = m \cdot m^{r(p-1)(q-1)} \bmod q = m (m^{q-1})^{r(p-1)} \bmod q =$   
 $= m (m^{\phi(q)})^{r(p-1)} \bmod q = m (1)^{r(p-1)} \bmod q = m \bmod q$   
 $\Rightarrow m^{ed} - m$  è divisibile per  $p$  e per  $q$ , allora è divisibile anche per  $n = p \cdot q$ , quindi  $m^{ed} - m \equiv 0 \bmod n$   
 $\Rightarrow m^{ed} \equiv m \bmod n = m^{ed} \equiv m \bmod n$  e perché  $m < n$  ho  $m \bmod n = m$
3.  $p, q$  dividono  $m$  non si verifica perché  $m < n$

**Sicurezza** Legata alla difficoltà di fattorizzare un numero arbitrario molto grande.

Fattorizzare  $\Rightarrow$  forzare RSA ok, è sufficiente per forzarlo

Fattorizzare  $\Leftarrow$  forzare RSA, non sappiamo se fattorizzare è necessario per forzarlo.

Il calcolo della radice in modulo  $m = \sqrt[n]{c} \bmod n$  difficile almeno quanto la fattorizzazione ( $n$  composto)

Calcolare  $\phi(n)$  direttamente da  $n$  è computazionalmente equivalente a fattorizzare  $n$

Significa che un problema si trasforma nell'altro in tempo polinomiale.

$$n = pq \longrightarrow \phi(n) = (p-1)(q-1), \text{ due riduzioni e un prodotto, polinomiale}$$

$$\phi(n) = (p-1)(q-1) \rightarrow \phi(n) = pq - (p+q) + 1 = n - (p+q) + 1$$

$$x_1 = p+q = n - \phi(n) + 1$$

$$\rightarrow (p-q)^2 = (p+q)^2 - 4pq = (p+q)^2 - 4n = x_1^2 - 4n$$

$$x_2 = p-q = \sqrt{x_1^2 - 4n}$$

$$\rightarrow p = \frac{x_1+x_2}{2}, q = \frac{x_1-x_2}{2}, \text{ polinomiale}$$

Ricavare  $d$  direttamente da  $\langle n, e \rangle$  sembra costoso quanto fattorizzare  $n$ . Come fattorizzare  $n$  intero? È un problema difficile ma non più come un tempo: hardware più potente e algoritmi più raffinati, siamo in grado di fattorizzare in tempo subesponenziale  $O(2^{\sqrt{b \cdot \log b}})$  con  $b = \log_2 n + 1$ , mentre il bruteforce richiede  $O(n)$  cioè  $O(2^b)$

Possiamo fattorizzare semiprimi fino a 768 bit, con l'algoritmo GNFS. Mentre per interi con strutture particolari ci sono algoritmi di fattorizzazione particolarmente efficienti.

La fattorizzazione e il logaritmo discreto non sono problemi NP-hard e si possono risolvere in tempo polinomiale su

macchine quantistiche.

Per avere una sicurezza in RSA pari ad un AES 128 bit devo usare un RSA con 3072 bit, per un AES 256 bit ho bisogno di RSA da 15360 bit.

Scegliere  $p$  e  $q$  molto grandi, per resistere a bruteforce.

Sia  $p - 1$  che  $q - 1$  devono avere un fattore primo molto grande, sennò  $n$  si fattorizza in fretta.

$\text{MCD}(p - 1, q - 1)$  deve essere piccolo (idealmente 2). Conviene scegliere  $p$  e  $q$  tali che  $(p - 1)/2$  e  $(q - 1)/2$  siano coprimi.

Non bisogna anche mai riutilizzare uno dei due primi per altri moduli, né sceglierli troppo vicini fra loro, sennò  $n^2$  sarà circa  $p^2$  o  $q^2$  e  $\sqrt{n}$  sarà vicino ai primi e basterà un bruteforce che cerca i fattori vicino a  $\sqrt{n}$

## Attacchi

### Attacchi con esponenti bassi

Esponenti  $e$  e  $d$  bassi sono attraenti perché accelerano cifratura e decifrazione. Ovviamente  $d$  deve essere scelto sufficientemente grande per evitare bruteforce.

Se  $m$  ed  $e$  sono così piccoli che  $m^e < n$ , allora **risulta facile trovare  $\sqrt[e]{c}$  poiché  $c = m^e$  e non interviene il modulo.**

### Attacchi a tempo

Si basano sul tempo di esecuzione dell'algoritmo di decifrazione. L'idea è determinare  $d$  analizzando il tempo impiegato per decifrare.

Quando si esegue l'esponenziazione modulare, si esegue una moltiplicazione ad ogni iterazione più un'**ulteriore moltiplicazione modulare per ciascun bit uguale a 1 in  $d$** . Come rimedio, si introduce un ritardo casuale per confondere l'attaccante.

### Attacco con $e$ troppo piccolo

Se  $e$  utenti scelgono lo stesso  $e$  piccolo e tutti ed  $e$  ricevono lo stesso messaggio  $m$  ottengo

$$\begin{aligned} c_1 &= m^e \bmod n_1 \\ c_2 &= m^e \bmod n_2 \\ &\vdots \\ c_e &= m^e \bmod n_e \end{aligned} \quad \forall i \text{ con } 1 \leq i \leq e \text{ e } m < n_i.$$

Poiché  $m \cdot m \cdot \dots \cdot m < n_1 \cdot n_2 \cdot \dots \cdot n_e = n$  so che  $m^e < n$ . Ipotizzo  $n_i$  coprimi fra loro, per il teorema cinese del resto  $\exists$  e si può facilmente calcolare un unico  $m'$  tale che  $m' < n$  e  $m' \equiv m^e \bmod n$

Dato che  $m' < n$  e  $m^e < n$ ,  $m' \bmod n = m^e \bmod n \Rightarrow m' = m^e \Rightarrow m = \sqrt[e]{m'}$

### Attacco con lo stesso valore di $n$

$\langle e_1, n \rangle, \langle e_2, n \rangle, \text{MCD}(e_1, e_2) = 1$

$\exists r, s \in \mathbb{Z} \mid e_1 r + e_2 s = 1 = \text{MCD}(e_1, e_2)$  e si trovano con l'algoritmo di Euclide esteso  $ax + by = \text{MCD}(a, b)$

Pongo  $r < 0, s > 0$ , Eve intercetta  $\begin{aligned} c_1 &= m^{e_1} \bmod n \\ c_2 &= m^{e_2} \bmod n \end{aligned} \Rightarrow m = m^1 =$

$$= m^{r e_1 + s e_2} = (m^{e_1} \bmod n)^r \cdot (m^{e_2} \bmod n)^s \bmod n = (c_1^r \cdot c_2^s) \bmod n = ((c_1^{-1})^{-r} \cdot c_2^s) \bmod n$$

Per  $c_1^{-1}$  calcolo l'inverso di  $c_1 \bmod n$ .  $(c_1^{-1})^{-r}$  e  $c_2^s$  con quadrature successive

$$\Rightarrow m = (c_1^{-1})^{-r} \cdot (c_2)^s \bmod n$$

## 5.3 Protocollo Diffie-Hellmann

Per esempio, RSA per scambiare la chiave e AES per proteggere la comunicazione.

**Alice** sceglie una chiave per AES ( $k[\text{session}]$ ) e la cifra con la chiave pubblica RSA di Bob. Cifra il messaggio con  $k[\text{session}]$  e invia i due crittogrammi a Bob.

$(C_{RSA}(k[\text{session}], k_{Bob}[\text{pub}]), C_{DES}(m, k[\text{session}]))$

**Bob** decifra il primo crittogramma con  $k_{Bob}[\text{prv}]$ , trova  $k[\text{session}]$  e decifra il secondo crittogramma

L'onere di creare la chiave di sessione è lasciato esclusivamente al mittente, ma la chiave deve essere generate in modo più possibile casuale.

**Protocollo** Alice e Bob si accordano pubblicamente su un numero primo  $p$  molto grande (migliaia di bit) e su un generatore  $g$  di  $Z_p^* = \{1, 2, \dots, p-1\} = \{g^k \bmod p \mid 1 \leq k \leq p-1\}$ .  $\exists g$  perché  $p$  è primo.

Alice e Bob possono anche scegliere di usare una coppia  $\langle p, g \rangle$  già disponibili. Non è richiesto che questa coppia sia mantenuta segreta.

Adesso il protocollo parte:

Alice	$\langle g, p \rangle$	Bob
Sceglie a caso $1 < x < p-1$ intero positivo, e calcola $A = g^x \bmod p$ Lo manda a Bob		Sceglie a caso $1 < y < p-1$ intero positivo, e calcola $B = g^y \bmod p$ Lo manda a Alice
	$\rightarrow A \rightarrow$ $\leftarrow B \leftarrow$	
Riceve B da Bob e calcola $k[\text{session}] = B^x \bmod p = g^{xy} \bmod p$		Riceve A da Alice e calcola $k[\text{session}] = A^y \bmod p = g^{xy} \bmod p$

### Attacchi

**Attacchi passivi**, il protocollo è **resistente**.

Il crittoanalista conosce  $p, g, A, B$ . Per calcolare  $k[\text{session}]$  deve trovare  $x$  o  $y$ , ma  $A = g^x \bmod p$  e  $B = g^y \bmod p$ .

Trovare  $x, y$  conoscendo  $A, B$  significa risolvere il logaritmo discreto che è un **problema difficile** quanto la fattorizzazione.

**Attacchi attivi**, il protocollo è **vulnerabile** ad attacchi del tipo MitM.

Alice	Eve	Bob
$A = g^x \bmod p \rightarrow$		$\leftarrow B = g^y \bmod p$
	Sottrae $A, B$ dal canale e il sostituisce con un suo $E = g^z \bmod p$ con $1 < z < p-1$ $\leftarrow$ La manda a entrambi $\rightarrow$	
$k[\text{session}] = E^x \bmod p = g^{xz} \bmod p$	Conosce sia $K_A = A^z \bmod p$ sia $K_B = B^z \bmod p$  $K_A \neq K_B$	$k[\text{session}] = E^y \bmod p = g^{yz} \bmod p$

## 5.4 Cifrario di Elgamal

Si basa sul logaritmo discreto come funzione one-way-trapdoor.

Alice  $\rightarrow m \rightarrow$  Bob

**Bob** sceglie  $p$  numero primo grande e  $g$  generatore per  $Z_g^*$

Sceglie  $2 \leq x \leq p-2$  come **chiave privata**,  $k[\text{prv}] = \langle x \rangle$

Calcola  $y = g^x \bmod p$

Pubblica  $k[\text{pub}] = \langle p, g, y \rangle$

**Alice**  $0 \leq m < p$

Si procura  $k[\text{pub}] = \langle p, g, y \rangle$

Sceglie a caso  $2 \leq r \leq p-2$  **segreto**

Calcola  $c = g^r \bmod p$ , cioè un numero casuale  $\in Z_p^*$  perché  $g$  generatore

Calcola  $d = (m \cdot y)^r \bmod p$

Invia a Bob  $\langle c, d \rangle$ , coppia di crittogrammi: il primo contiene protetta l'informazione su  $r$ , e  $d$  contiene il messaggio  $m$

**Bob** riceve  $\langle c, d \rangle$  e decifra:

$$m = \frac{d}{c^x} \bmod p = d \cdot (c^x)^{-1} \bmod p \text{ (dove la frazione indica la moltiplicazione per l'inverso)}$$

**Correttezza**  $m = \frac{d}{c^x} \bmod p = \frac{y^r \cdot m}{c^x} \bmod p = \frac{(g^{x^r}) \cdot m}{(g^r)^x} \bmod p = m \bmod p = m$  perché  $m < p$

**Attacchi** Eve conosce  $p, g, y, c, d$ , cioè tutto tranne  $x$  e  $r$ .

Se conosce  $x$  calcola  $m = \frac{d}{c^x} \bmod p$

Se conosce  $r$  calcola  $m = \frac{d}{y^r} \bmod p = \frac{m \cdot y^r}{y^r} \bmod p = m$





## Capitolo 6

# Elliptic Curve Cryptography

Equivalenze di costo degli attacchi		
AES	RSA, DH, Elgamal	ECC
128 bit	3072 bit (di $n, p$ )	256 bit
256 bit	15000 bit	512 bit

**Cosa sono** Curve algebriche descritte da equazioni simili a quelle usate per il calcolo degli archi delle ellissi. 1985 da Miller e Kobitz, propongono di prendere la cifratura a chiave pubblica e modificarli sostituendo solo le operazioni: invece che algebra modulare usare punti delle curve ellittiche.

**Definizione generale** Campo  $K$ , insieme di punti  $(x, y) \in K^2 \mid y^2 + axy + by = x^3 + cx^2 + dx + e$  con  $a, b, c, d, e \in K$ . Se la caratteristica di  $K \neq 2, 3$  allora esiste la forma normale di Weierstrass  $y^2 = x^3 + ax + b$  con  $a, b \in K$ .

La **caratteristica** di un campo è il numero di volte che io devo sommare l'elemento neutro moltiplicativo (1) per ottenere l'elemento neutro additivo (0). Ad esempio, negli interi modulo  $p$  primo, la caratteristica è  $p$ :  $p \cdot 1 \bmod p = 0$ . In  $\mathbb{R}$  la caratteristica è 0, non esiste.

Con caratteristica  $\neq 2, 3$ , la curva ellittica può essere descritta da

$$E_K(a, b) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{0\}$$

Noi prenderemo  $K = \mathbb{R}$ , cioè  $E(a, b) = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b\} \cup \{0\}$ .

La richiesta è che  $x^3 + ax + b$  **non abbia radici multiple**, cioè **assumiamo che**  $4a^3 + 27b^2 \neq 0$  (discriminante). Questo garantisce l'esistenza della tangente in ogni punto della curva ellittica.

**Simmetria orizzontale** Dato  $P = (x, y) \in E(a, b)$ , quindi  $x, y$  soddisfano  $y^2 = x^3 + ax + b \Rightarrow -P = (x, -y) \in E(a, b)$  infatti  $(-y)^2 = y^2 = x^3 + ax + b$ .

Per il punto all'infinito si pone  $O = -O$



# Capitolo 7

## Esercizi

### 7.1 Complessità e randomizzazione

**Esercizio 1** Un sistema crittografico impiega chiavi private di 46 bit. Per decifrare un messaggio  $m$  data la chiave, un programma in assembler impiega un ciclo di 128 istruzioni ripetuto in media tante volte quanti sono i bit che costituiscono  $m$ . Impiegando un calcolatore che esegue un'operazione assembler in un tempo medio di 10ns, indicare in ordine di grandezza quanti anni sarebbero necessari in media per condurre un attacco esaustivo sulle chiavi per un messaggio  $m$  di 1000 bit. Indicare i calcoli eseguiti.

#### Svolgimento

$$\# \text{ chiavi} = 2^{46}$$

$$\# \text{ operazioni per chiave} = 128 \cdot |m|$$

$$|m| = 1000 \text{ bit} = 10^3 \text{ bit}$$

$$1\text{ns} = 10^{-9}\text{s}$$

$$\Rightarrow t = 2^{46} \cdot 128 \cdot 10^3 \cdot 10 \cdot 10^{-9}\text{s} = 2^{46} \cdot 2^7 \cdot 10^{-5}\text{s} = 2^{53} \cdot 10^{-5}\text{s} = 2^3 \cdot 2^{50} \cdot 10^{-5}\text{s} \text{ e dato che } 2^{10} \simeq 10^3 \\ \Rightarrow \simeq 2^8 \cdot (10^3)^5 \cdot 10^{-5}\text{s} = 8 \cdot 10^{10}\text{s} \simeq 2500 \text{ anni}$$

**Esercizio 2** Si vuole generare una sequenza di bit pseudocasuali utilizzando il generatore BBS basato sulla legge:

$$x_i = x_{i-1}^2 \bmod n \quad b_i = 1 \Leftrightarrow x_{m-i} \text{ è dispari}$$

1. **Scegliere**  $n = 11 \cdot 23$  e verificare che 11 e 23 soddisfano i requisiti del BBS
2. Sia  $M$  la propria matricola. Porre  $y = M \bmod 100$  e  $x_0 = y^2 \bmod n$  e **indicare** una sequenza di 10 bit generati, riportando i calcoli
3. **Discutere** se il generatore è crittograficamente sicuro

#### Svolgimento

1. Verificare che  $11 \bmod 4 = 3$  (ok) e  $23 \bmod 4 = 3$  (ok)  
Verificare che  $2\lfloor \frac{11}{4} \rfloor + 1 = 2 \cdot 2 + 1 = 5$  e  $2\lfloor \frac{23}{4} \rfloor + 1 = 11$  siano primi fra loro (sono primi entrambi, ok)
2. Usiamo  $M = 123456$ ,  $M \bmod 100 = 56$  e  $11 \cdot 23 = 253$

$$x_0 = 56^2 \bmod 253 = 100 \rightarrow 0$$

$$x_1 = 100^2 \bmod 253 = 133 \rightarrow 1$$

$$x_2 = 133^2 \bmod 253 = 232 \rightarrow 0$$

$$x_3 = 232^2 \bmod 253 = 188 \rightarrow 0$$

$$x_4 = 188^2 \bmod 253 = 177 \rightarrow 1$$

$$x_5 = 177^2 \bmod 253 = 210 \rightarrow 0$$

$$x_6 = 210^2 \bmod 253 = 78 \rightarrow 0$$

$$x_7 = 78^2 \bmod 253 = 12 \rightarrow 0$$

$$x_8 = 12^2 \bmod 253 = 144 \rightarrow 0$$

$$x_9 = 144^2 \bmod 253 = 243 \rightarrow 1$$

$$\longrightarrow 1000010010$$

**Esercizio 3** Sia  $C$  una sequenza ottenuta rappresentando in binario ciascuna delle due cifre centrali del numero di matricola del candidato, prendendo per ciascuna di esse i tre bit meno significativi, concatenando questi due gruppi di bit e aggiungendo 1 in testa.

1. Eseguire  $37^C \bmod 100$  per esponenziazioni successive **indicando** i calcoli eseguiti
2. **Spiegare** perché tale metodo di calcolo è considerato efficiente

**Svolgimento** Con  $M = 123456$ ,  $3 = 011$  e  $4 = 100$   
 $C = 1011100 = 64 + 16 + 8 + 4 = 92$

$$1. 37^{92} \bmod 100 = 37^{64+16+8+4} \bmod 100$$

$$37^4 \bmod 100 = 69^2 \bmod 100 = \underline{61}$$

$$37^8 \bmod 100 = 61^2 \bmod 100 = \underline{21}$$

$$37^{16} \bmod 100 = 21^2 \bmod 100 = \underline{41}$$

$$37^{32} \bmod 100 = 41^2 \bmod 100 = 81$$

$$37^{64} \bmod 100 = 81^2 \bmod 100 = \underline{61}$$

$$\Rightarrow 37^{92} \bmod 100 = (61 \cdot 41 \cdot 21 \cdot 61) \bmod 100 = 81$$

2. Perché esegue un numero di moltiplicazioni logaritmico nel valore dell'esponente (dunque lineare nella dimensione)

**Esercizio 4** Applicando l'algoritmo Miller-Rabin, individuare un numero  $N$  primo di tre cifre decimali con probabilità di errore minore di  $\frac{1}{50}$ , spiegando il procedimento eseguito.

**Svolgimento**  $N = 113$ , ho  $\frac{1}{4^k} < \frac{1}{50}$  per  $k = 3$ , quindi servono 3 testimoni  $y$  scelti a caso  $\in [2, 112]$   
 Pongo  $y = 3$

$$1. \text{MCD}(113, 3) = \text{MCD}(3, 113 \bmod 3) = \text{MCD}(2, 3 \bmod 2) = \text{MCD}(1, 0) = 1 \text{ ok}$$

$$2. N = 113$$

$$N-1 = 112 = 2^4 \cdot 7, w = 4 \text{ e } z = 7$$

$$3^7 \bmod 113 = 3^{1+2+4} \bmod 113 =$$

$$3^2 \bmod 113 = 9$$

$$3^4 \bmod 113 = 9^2 \bmod 113 = 81$$

$$= (3 \cdot 9 \cdot 81) \bmod 113 = 40 \neq -1, \text{ bisogna proseguire nella valutazione di } P2$$

$$0 \leq i \leq w - 1 = 3$$

$$i = 0 \quad 3^{2^0 \cdot 7} \bmod 113 = 3^7 \bmod 113 = 40 \neq -1 \text{ (40 preso dal precedente risultato)}$$

$$i = 1 \quad 3^{2^1 \cdot 7} \bmod 113 = (3^7)^2 \bmod 113 = 40^2 \bmod 113 = 18 \neq -1 \text{ (40 preso dal precedente risultato)}$$

$$i = 2 \quad 3^{2^2 \cdot 7} \bmod 113 = (18)^2 \bmod 113 = 98 \neq -1 \text{ (18 preso dal precedente risultato)}$$

$$i = 3 \quad 3^{2^3 \cdot 7} \bmod 113 = (98)^2 \bmod 113 = -1 \text{ ok (98 preso dal precedente risultato)}$$

Per gli altri 2 valori di  $y$  il procedimento è analogo

## 7.2 Cifrari Storici

**Esercizio 1** Decifrare i seguenti crittogrammi

1. YMNXCJCJWHNXCJNXCJFXD (Cifrario Cesare, chiave  $k \neq 3$ )
2. REXETSIH ONSICESI UCIFTFID REHTLIET (Cifrario a permutazione semplice,  $h = 8$ )

**Svolgimento**

$$1. \text{ Con } k = 21 \text{ diventa THISEXERCISEISEASY}$$

$$2. \text{ Con } \pi = \{5, 8, 7, 6, 4, 3, 2, 1\} \text{ diventa THISEXER CISEISNO TDIFFICU LTEITHER}$$

**Esercizio 2** Dato un cifrario affine (mod 26), si fa un attacco di tipo chosen plain-text usando il testo *hahaha*. Il testo cifrato è *nonono*. Determinare la funzione di cifratura.

**Svolgimento** Un cifrario affine è un cifrario che associa a  $\text{pos}(X) = a \cdot \text{pos}(Y) + b$   
 Bisogna trovare  $a, b \mid \text{pos}(n) = a \cdot \text{pos}(h) + b \bmod 26 \wedge \text{pos}(o) = a \cdot \text{pos}(a) + b \bmod 26$   
 con  $\text{pos}(n) = 13, \text{pos}(h) = 7, \text{pos}(o) = 14$  e  $\text{pos}(a) = 0$   

$$\begin{cases} 13 = a \cdot 7 + b \bmod 26 \Leftrightarrow a = 11 \\ 14 = a \cdot 0 + b \bmod 26 \Leftrightarrow b = 14 \end{cases}$$
 ottenendo i due parametri  $a = 11$  e  $b = 14$  che danno il cifrario  
 $\text{pos}(Y) = (11 \cdot \text{pos}(X) + 14) \bmod 26$

**Esercizio 3** Se nei cifrari affini si lavorasse in modulo 27 invece che modulo 26, quante sarebbero le chiavi possibili? E in modulo 29?

**Svolgimento** Con un alfabeto di 27 caratteri,  $a$  deve essere primo con  $27 = 3^3$   
 $\rightarrow a$  può assumere i valori da 1 a 26 non multipli di 3  
 $\rightarrow \phi(27) = \phi(3^3) = 2 \cdot 3^2 = 18$  (tramite la **funzione di Eulero**  $\phi(p^k) = (p-1)p^{k-1}$  con  $p$  primo)  
 $\rightarrow b$  può assumere tutti i valori  $\in [0, 26]$   
 $\Rightarrow \# \text{ chiavi} = 18 \cdot 27 - 1 = 485$  (il -1 esclude la coppia  $(a, b) = (1, 0)$  che lascia invariato il messaggio)

Con un alfabeto di 29 caratteri: 29 è primo, quindi  $a$  può assumere tutti i valori  $\in [1, 28]$  ( $\rightarrow \phi(29) = 28$ ) e  $b$  tutti i valori  $\in [0, 28]$   
 $\Rightarrow \# \text{ chiavi} = 28 \cdot 29 - 1 = 811$

**Esercizio 4** Questo esercizio ha lo scopo di dimostrare che un cifrario affine iterato ha la stessa sicurezza di un cifrario singolo.

Si considerino due cifrari affini:

$$C_1(x) = (a_1 \cdot x + b_1) \bmod 26$$

$$C_2(x) = (a_2 \cdot x + b_2) \bmod 26$$

**Dimostrare** che  $\exists$  un cifrario affine  $C_3 \mid C_3(x) = C_2(C_1(x))$

**Svolgimento**  $C_2(C_1(x)) = (a_2 \cdot C_1(x) + b_2) \bmod 26 = (a_2 \cdot (a_1 \cdot x + b_1) + b_2) \bmod 26$   
 $= (a_1 a_2 x + a_2 b_1 + b_2) \bmod 26 = (a_3 \cdot x + b_3) \bmod 26$   
 Con  $a_3 = a_1 a_2 \bmod 26, b_3 = a_2 b_1 + b_2 \bmod 26$

**Esercizio 5** Il crittogramma  $c = \text{MBR OJFGA SWNTE CNK QJDIL NURW MBR XHMR}$  è ottenuto cifrando  $m = \text{THE QUICK BROWN FOX JUMPS OVER THE GATE}$  con un cifrario a sostituzione monoalfabetica completo.

1. Quanta informazione relativa alla chiave si può determinare conoscendo la coppia  $m, c$ ?
2. Quante chiavi differenti potrebbero essere state usate per cifrare il messaggio  $m$ ?
3. **Decifrare** il crittogramma  $\text{MBR TRHLRP WHE HTHV CWND PNEYNE ZNN}$ , che è stato cifrato usando la stessa chiave usata per cifrare  $m$

**Svolgimento**

1. Parte della permutazione che definisce il cifrario.  
 Più precisamente, si trova l'immagine cifrata di 22 caratteri su 26.
2. 24 chiavi  
 Infatti mancano le corrispondenze per 4 caratteri, e se ne potrebbero costruire  $4! = 24$  differenti
3. THE WEASEL RUN AWAY FROM LONDON ZOO

**Esercizio 6** Usando il metodo di Vigenère, **cifrare** il messaggio CRITTOGRAFIA impiegando come chiave le prime 4 lettere del proprio cognome. **Spiegare** inoltre come tale cifrario possa essere attaccato.

**Svolgimento** Si incrocia la lettera del messaggio con la lettera del crittogramma sulla tabella di Vigenère per trovare la lettera cifrata. Ad esempio, alla colonna C e riga M corrisponde la lettera O.

C R I T T O G R A F I A

M A T T M A T T M A T T

→ O A B M F O Z K M F B T

Per la spiegazione, vedi appunti.

**Esercizio 7** Si deve cifrare il messaggio APPELLODIFEBBRAIO impiegando come chiave una permutazione arbitraria e segreta delle 26 lettere dell'alfabeto.

1. **Mostrare** la permutazione scelta e il crittogramma ottenuto
2. **Calcolare** il numero di prove necessarie per condurre un attacco esaustivo sulle chiavi
3. **Discutere** la possibilità di un attacco più efficiente confrontandolo con quello del punto 2

**Svolgimento**

1. Ad esempio, DOAIIPFAPEREBBLOL

2. In generale  $26! - 1$

Ma per decifrare il crittogramma ottenuto cifrando APPELLODIFEBBRAIO occorrono meno prove, perché il crittogramma contiene 10 lettere diverse tra loro da decifrare.

$$\Rightarrow \# \text{ prove} = 26 \cdot 25 \cdot \dots \cdot 17 = \frac{26!}{16!} \simeq 2 \cdot 10^{13}$$

3. Crittoanalisi statistica

## 7.3 Cifrari Perfetti

**Esercizio 1** Sia  $M$  il numero di matricola del candidato. Si converta  $M$  in una sequenza binaria  $B$  trasformando ordinatamente in binario ogni cifra decimale di  $M$ , prendendo per ciascuna di esse i tre bit meno significativi e concatenando tali gruppi di tre bit.

1. **Indicare** la sequenza  $B$ , **proporre** una chiave  $K$  di 18 bit ottenuta lanciando idealmente una moneta e **trasformare**  $B$  mediante One-Time Pad usando  $K$
2. **Spiegare** se il cifrario può ritenersi sicuro per messaggi binari di lunghezza multipla di 18, utilizzando come chiave una ripetizione di  $K$  per il numero di volte necessario

**Svolgimento**

1.  $B = 101011000010101111$   
 $K = 010111001110111011$   
 $C \Rightarrow 111100001100010100$

2. Il riutilizzo di  $K$  rende il procedimento indicato non sicuro quanto il one-time pad

**Esercizio 2** In un cifrario  $A$  esistono un messaggio  $m$  e un crittogramma  $c$  |  $P(M = m) = p \leq \frac{1}{4}$ ,  $P(C = c) = 1 - p$ . **Spiegare** se  $A$  può essere un cifrario perfetto e le conseguenze per un crittoanalista per la coppia  $m, c$  indicata.

**Svolgimento**

**Esercizio 3** **Spiegare** con precisione matematica e proprietà di linguaggio perché il cifrario One-Time Pad su messaggi di  $n$  bit non può essere ritenuto perfetto se la chiave non è scelta perfettamente a caso.

**Svolgimento** Se ho una chiave con una qualche regolarità, lo xor farebbe filtrare tale proprietà sul crittogramma.

**Esercizio 4** Nel codice one-time pad si sostituisca  $\oplus$  con  $\vee$  o con  $\neg\oplus$ .  
**Spiegare**, nei due casi, se il protocollo funziona con le stesse proprietà del codice originale.

**Svolgimento**

**Esercizio 5** Qual è lo svantaggio principale del cifrario one-time pad?

**Svolgimento** La chiave: deve essere perfettamente casuale e non venire riutilizzata.

**Esercizio 6** Nel one-time pad si consideri una coppia arbitraria messaggio-crittogramma  $m, c$  di  $n$  bit.  
**Spiegare** quanto vale  $P(M = m, C = c)$  (nota: è la probabilità dell'intersezione degli eventi, non quella condizionale)

**Svolgimento**

## 7.4 Cifrari Simmetrici

**Esercizio 1** Sia  $C$  una sequenza ottenuta rappresentando in binario ciascuna delle due cifre centrali del numero di matricola del candidato, prendendo per ciascuna di esse i tre bit meno significativi e concatenando questi due gruppi di tre bit. Nella fase  $i$ -esima del DES,  $C$  costituisca la parte iniziale della sequenza in ingresso della S-box

1. **Indicare** la sequenza  $C$
2. **Indicare**, con interi crescenti da 1 a 32, la sequenza POS di posizioni dei bit di  $D[i]$  influenzati da  $C$ , **spiegando** com'è stato ottenuto il risultato
3. Posto che la parte sinistra di  $S[i - 1]$  del messaggio entrante nella fase  $i$  sia una sequenza di 1, **indicare** il valore dei bit di  $D[i]$  di cui al punto 2, **riportando** i calcoli eseguiti

**Svolgimento**

1. 000010
2. Passando attraverso  $S_1$ ,  $C$  dà in output 0100 (prendo i due bit esterni 00 per l'indice  $x$  e i rimanenti 0001 per l'indice  $y$ , trovando 04 nella tabella che in binario è 0100)  
 Questi bit andranno rispettivamente in posizione 9, 17, 23 e 30 di  $D[i]$ , seguendo la tabella P (01 è in posizione 9 e così via). Quindi  $D[9] = 0$ ,  $D[17] = 1$ ,  $D[23] = 0$  e  $D[30] = 0$
3. Con  $S[i - 1]$  eseguo lo  $\oplus$  (xor) con i bit in uscita da P. Quindi  $D[9] = 1 \oplus 0 = 1$ ,  $D[17] = 1 \oplus 1 = 0$ ,  $D[23] = 1 \oplus 0 = 1$  e  $D[30] = 1 \oplus 0 = 1$

**Esercizio 2** Si trasformi il DES complementando tutte le uscite della s-box.  
 Sia  $M$  il proprio numero di matricola. Si converta  $M$  in una sequenza binaria  $B$  trasformando ordinatamente in binario ogni cifra decimale di  $M$  e prendendo per ciascuna i tre bit meno significativi. Si estenda  $B$  fino ad avere 48 bit, aggiungendo zeri a destra: sia tale sequenza l'uscita del blocco EP del DES con chiave  $k[0] = 1010 \dots 10$

1. **Indicare** la sequenza  $B$
2. Nella fase 1 del DES, **determinare** il valore dei primi 4 bit a sinistra in uscita dalla s-box, spiegando come è stato ottenuto il risultato
3. **Commentare** se il DES così modificato appaia o meno palesemente meno sicuro della versione standard

**Svolgimento**

1.  $B = 101\ 011\ 000\ 010\ 101\ 111\ 000\ 000\ 000\ 000\ 000\ 000\ 000\ 000\ 000$
2. Nella  $S_i$  entrano 6 bit, quindi per vedere i primi 4 bit prodotti bisogna usare la  $S_1$  con i primi 6 bit di  $B$ , cioè con 1 0101 1. Con i bit esterni si indicizza  $x$ , in questo caso con valore 3 uso la quarta riga, e con i 4 bit interni si indicizza  $y$ , in questo caso con valore 5, ottenendo il valore 09, che quindi consiste nei bit 1001. Per la modifica proposta, bisogna complementare ogni bit, ottenendo 0110.
- 3.

**Esercizio 3** Nella fase  $i$ -esima del DES, siano 000011 i primi 6 bit a sinistra in ingresso alla s-box.

1. **Indicare** (con interi crescenti tra 1 e 32) la sequenza POS di posizioni dei bit di  $S[i+1]$  influenzati da questi 6 bit, spiegando come è stato ottenuto il risultato.
2. Siano  $c_1 c_2 \dots$  i bit di  $S[i-1]$  nelle posizioni indicate in POS (le stesse quindi di  $S[i+1]$ ).  $c_1 c_2 \dots$  rappresentino in binario il numero di consonanti presenti nel nome e cognome del candidato. **Indicare** il valore dei bit di  $S[i+1]$  nelle posizioni POS spiegando come è stato ottenuto il risultato.

### Svolgimento

1. Avendo 1 0001 1 come bit, ottengo 12 cioè 1100 come bit.  
Ogni bit andrà, secondo la tabella P, rispettivamente in posizione 9, 17, 23, 31 di  $D[i]$ , che diventerà  $S[i+1]$ .
2. La sequenza data da  $c$  è 1000.  
Bisogna fare lo  $\oplus$  tra  $S[i-1] = 1000$  e  $D$  attuale = 1100. Quindi

$$S[9] = 1 \oplus 1 = 0$$

$$S[17] = 0 \oplus 1 = 1$$

$$S[23] = 0 \oplus 0 = 0$$

$$S[31] = 0 \oplus 0 = 0$$

ottenendo 0 1 0 0 rispettivamente nelle posizioni 9, 17, 23, 31.

**Esercizio 4** La s-box del cifrario AES è composta da 16 blocchi con 8 ingressi e 8 uscite ciascuno. Qual è il numero totale di possibili funzioni che si potrebbero scegliere per costruire ciascun blocco?

**Svolgimento** Per ognuna delle  $2^8$  configurazioni di input, posso scegliere  $2^8$  configurazioni in output. Quindi ho  
 $\# \text{ funzioni} = (2^8)^{2^8} = 2^{8 \cdot 2^8}$

**Esercizio 6** La proprietà di non linearità di qualsiasi cifratura a blocchi è fondamentale per la sicurezza. Infatti, si supponga di avere una cifratura lineare a blocchi  $Cl$  che figura blocchi di 128 bit di testo in chiaro in 128 bit di testo cifrato, usando una chiave  $k$  la cui lunghezza è irrilevante. Dunque, ogni coppia di messaggi  $m_1$  e  $m_2$  risulta  $Cl(m_1 \oplus m_2, k) = Cl(m_1, k) \oplus Cl(m_2, k)$

**Descrivere** come un avversario che abbia 128 testi cifrati scelti possa decifrare qualsiasi testo cifrato senza conoscere la chiave  $k$ .

**Svolgimento** Prendo  $c$  il crittogramma di un generico  $m$ ,  $c = Cl(m, k)$ . Posso rappresentare  $c = \bigoplus_{i:c_i=1} e^{(i)}$  dove  $e^{(i)}$  ha un solo bit a 1 in posizione  $i$ , e gli altri 127 bit a 0.

Per esempio  $c = 1011 = 1000 \oplus 0010 \oplus 0001 = e^{(1)} \oplus e^{(3)} \oplus e^{(4)}$

Sfruttiamo le proprietà delle funzioni di cifratura e decifrazione:  $m = D(c, k) = D(\bigoplus_{i:c_i=1} e^{(i)}, k) = \bigoplus_{i:c_i=1} D(e^{(i)}, k)$

Si chiede la decifrazione dei 128 testi cifrati  $e^{(i)}$ ,  $i \in [1, 128]$ ,  $f^{(i)} = D(e^{(i)}, k)$

Si può decifrare qualsiasi crittogramma  $c$  anche senza conoscere  $k$ :  $m = \bigoplus_{i:c_i=1} f^{(i)}$

**Esercizio 7** DESX è un cifrario proposto da Rivest per proteggere il DES dagli attacchi esaurienti. DESX usa una chiave segreta  $w$  di 64 bit, oltre alla chiave DES  $k$  di 56 bit, e opera così:

$$C_{DESX}(m, k, w) = w \oplus C_{DES}(m \oplus w, k)$$

Mostrare come eseguire la decifrazione.

**Svolgimento**  $c = C_{DES}(m \oplus w, k) \Leftrightarrow c \oplus w = C_{DES}(m \oplus w, k)$   
 $\Leftrightarrow D_{DES}(c \oplus w, k) = D_{DES}(C_{DES}(m \oplus w, k))$  ma  $D_{DES}(C_{DES}(m \oplus w, k)) = m \oplus w$  perché DES è un cifrario corretto  
 Quindi  $\Leftrightarrow m \oplus w = D_{DES}(c \oplus w, k) \Leftrightarrow m = w \oplus D_{DES}(c \oplus w, k)$