Appunti di crittografia

Riccardo Pietrucci

18 aprile 2006

Indice

1 Cenni Storici

1.1 Introduzione

La prima persona che usò la crittografia fu Giulio Cesare. Egli doveva inviare messaggi ma non si fidava dei messaggeri, così inventò un metodo per codificare quei messaggi: solo il destinatario prestabilito — che conosceva il metodo per decodificare il messaggio — poteva leggerli.

Definizione 1.1. *La* crittografia *è l'arte che crea ed usa i sistemi di crittografia*

Definizione 1.2. *Un* sistema di crittografia *è un metodo per rendere illeggibili i messaggi, in modo da renderli decodificabili solo dal destinatario prestabilito.*

I sistemi di crittografia sono chiamati anche *sistemi di cifratura*.

Definizione 1.3. *La* crittoanalisi *è l'arte di scardinare i sistemi di cifratura*

Definizione 1.4. *La* crittologia *è la scienza che studia la crittografia e la crittoanalisi*[1]

Il messaggio originale è chiamato *testo in chiaro*, ed il messaggio codificato è chiamato *testo cifrato*. La *cifratura* è la procedura che converte il testo in chiaro in testo cifrato. Il procedimento inverso è chiamato *decifratura*.

1.2 Crittografia e steganografia

Il pericolo di intercettazione da parte dei nemici è stato sicuramente il principale motivo della ricerca di codici e di tecniche di alterazione di un messaggio al fine di a renderlo comprensibile solo alle persone autorizzate.

Una delle prime tecniche di comunicazione segrete, basata sull'occultamento del messaggio, si chiama *steganografia*.

Un esempio di steganografia era utilizzato nell'antica Persia. Ci è stato descritto da Erodoto nel 400 a.C.. Consisteva nel rapare i capelli di uno schiavo e nel scrivergli il messaggio sulla testa. Lo schiavo si recava poi dal destinatario del messaggio dopo che gli erano ricresciuti i capelli e il messaggio era recuperato rapandoglieli nuovamente. Un ulteriore esempio si ha nel XVI secolo, quando lo scienziato italiano Giambattista Della Porta spiegò come comunicare tramite un uovo sodo. Si prepara un inchiostro con 30 grammi di allume in mezzo litro d'aceto e lo si usa per scrivere sul guscio. La soluzione penetra nel guscio, che è poroso, senza lasciar traccia, e tinge l'albume solidificato; quest'ultimo potrà essere letto sbucciando l'uovo.

[1] dal greco kryptos, che significa 'nascosto' e logos, che significa 'discorso, parola'

Parallelamente allo sviluppo della steganografia si evolve la *crittografia*. La crittografia non mira a nascondere il messaggio ma il suo significato. Per rendere incomprensibile un testo, lo si altera per mezzo di un procedimento concordato dal mittente e dal destinatario. Quest'ultimo può invertire il procedimento e ricavare il messaggio originale. Il vantaggio della crittografia è che se il messaggio viene intercettato risulta incomprensibile e quindi inutilizzabile.

Come esempio abbiamo il codice di Cesare (100–1 d.C), in cui abbiamo una traslazione di quattro caratteri, e risultava quindi incomprensibile se intercettato.

1.3 Crittografia antica

Le più antiche notizie sicure sull'origine della crittografia sono probabilmente quelle sulla *scitala lacedemonica*. Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio; sul nastro si scriveva per colonne parallele all'asse del bastone, lettera per lettera, il testo segreto. Tolto il nastro dal bastone, il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la comprensione senza un secondo bastone uguale al primo.

Nel Vecchio Testamento, si possono ritrovare tre principali scritture segrete. Tra queste, l'Atbash, è stato ideato dal popolo ebraico e consisteva nel capovolgere l'alfabeto. Di conseguenza la prima lettera diventava l'ultima e l'ultima la prima e così per tutte le altre lettere dell'alfabeto.

Nel 1466 Leon Battista Alberti, nel suo Trattato, ha proposto un disco composto di due cerchi concentrici di rame. Uno esterno fisso di diametro maggiore sul quale sono riportate le lettere dell'alfabeto in chiaro e uno interno mobile per le lettere dell'alfabeto cifrante. Fissata una lettera maiuscola come chiave, ad esempio B, si deve spostare il disco mobile interno in modo da far corrispondere la B con un simbolo particolare del disco interno.

Nel 1586 la crittanalisi fu usata dallo spymaster Francis Walsingham per implicare Maria Stuart nel Complotto Babington per uccidere Elisabetta I d'Inghilterra. Maria Stuart fu giustiziata.

Quasi tutte le comunicazioni tedesche venivano cifrate con una macchina chiamata Enigma. Questa macchina è una nobile rappresentante dei cifrari a rotore, utilizzati fino all'introduzione di cifrari elettronici e microelettronici. Per rompere Enigma (alcuni dettagli della soluzione sono tenuti segreti fino ad oggi) Turing si servì di gigantesche macchine chiamate Colossi, che possono considerarsi i precursori dei moderni calcolatori elettronici. Turing è autore di ricerche estremamente importanti sul concetto logico-matematico di calcolabilità: lo strumento che egli ha proposto per affrontare il problema è noto oggi col nome di macchina di Turing.

2 Crittografia classica (o a chiave segreta

2.1 Crittosistemi

Definizione 2.1. *Si definisce* crittosistema *la quaterna* $(\mathfrak{M}, \mathfrak{C}, f, f^{-1})$ *dove* f *è una trasformazione crittografica tale che siano verificate le proprietà:*

$$\begin{aligned} f &: \mathfrak{M} \to \mathfrak{C} \textit{(iniettiva)} \\ f &: \mathfrak{M} \to f(\mathfrak{M}) \textit{(biettiva)} \\ f^{-1} &: f(\mathfrak{M}) \to \mathfrak{M} \end{aligned}$$

Definizione 2.2. *Una funzione* $f : A \to B$ *si dice* iniettiva *se vale, in modo equivalente:*

$$\begin{aligned} \forall x, x' \in A, \quad x \neq x' \quad &\Rightarrow f(x) \neq f(x') \\ \forall x, x' \in A, \quad f(x) = f(x') \quad &\Rightarrow x = x' \end{aligned}$$

Definizione 2.3. *Una funzione* $f : A \to B$ *si dice* suriettiva *se tutti gli elementi sono coperti, ovvero se:* $\forall y \in B \; \exists x \in A \Rightarrow y = f(x)$

Definizione 2.4. *Una funzione* $f : A \to B$ *si dice* iniettiva *se è sia iniettiva che suriettiva*

2.1.1 Cifrari monoalfabetici

Nel codice di Cesare abbiamo una traslazione di quattro caratteri. Perciò se l'alfabeto in chiaro è ABCDEFGH... allora l'alfabeto crittato sarà DEFGHIJK.... Le combinazioni sono rappresentabili attraverso una circonferenza.

Quando si arriva alla fine dell'alfabeto si calcola il mod 26 della lettera. Quindi

Definizione 2.5. *Il* codice di Cesare *è un algoritmo di codifica in cui la trasformazione crittografica è una traslazione di chiave 3.*

Quindi sia l'alfabeto in chiaro che quello crittato hanno un dominio di 26 numeri interi:

$$\mathfrak{M} = \mathfrak{C} = \mathbb{Z}_{26}$$

Esempio 2.1 A quale classe di equivalenza appartiene 35?

$$[35]_{26} = [9]_{26} \qquad (35 \bmod 26)$$

Esempio 2.2 Codificare la stringa "Codice di Cesare"

$\mathfrak{M}$	: CODICE DI CESARE
$\mathfrak{C}$	: FRGLFH GL FHVDUH

Inoltre se $\tau_a, a \in \{0, \ldots, 25\}$ è la traslazione corrispondente ad una qualunque chiave a, si ha:

$$\begin{aligned} \tau_3 : \mathfrak{M} &\to \mathfrak{C} \\ x &\to x + 3 \end{aligned}$$

Esistono 26 chiavi distinte (o classi di equivalenza), poiché ci sono 26 possibilità di traslare l'alfabeto in chiaro:

$$\tau_3(x) = (x + 3) \bmod 26$$

Quindi avremo 26 distinte classi di equivalenza:

$$\begin{aligned} \mathbb{Z}_{26} &= \{\overline{0}, \ldots, \overline{25}\} \\ &= [0], \ldots, [25] \end{aligned}$$

In altri contesti, quando si ha un messaggio molto lungo, si adotta l'*analisi di frequenza*.

Il *codice dei monaci* sostituivano la prima con l'ultima, la seconda con la penultima, ...

Definizione 2.6. *Gli alfabeti* nomenclatori *(o* nomenclatura*) sono alfabeti cifranti composti non solo da letter ma anche da numeri o simboli diversi*

2.1.2 Cifrari polialfabetici

Il *cifrario di Vigenère* considera una matrice 26×26, dove:

- le colonne identificano tutte le possibili traslazioni
- le righe identificano tutte le possibili posizioni assunte dall'alfabeto (traslato)

Il sistema prevede i seguenti passaggi:

1. la scelta di un messaggio $\mathfrak{M}$

Esempio 2.3 Codificare il messaggio "Cifrario" con il cifrario di Vigenère utilizzando come chiave "Tavola"

$\mathfrak{M}$	: CIFRARIO
	: TAVOLATAVOLA
$\mathfrak{C}$	: VIAF....

2. la scelta di una chiave K

3. $\forall m \in \mathfrak{M}, \forall k \in K$, viene scelta nella matrice la colonna m e la riga k, eventualmente ripetendo più volte la chiave K

Fu utilizzato a lungo, ma aveva un problema di sicurezza. Si consideri la coppia $\mathfrak{M}-K$:

```
UNCALCOLOFACILEEUNPRODOTTO
REBUSREBUSREBUSREBUSREBUSR
```

Un messaggio $\mathfrak{M}$ spesso contiene elementi uguali (l'articolo 'un' dell'esempio), e potrebbe succedere che gli elementi ripetuti siano intere coppie $\mathfrak{M} - K$ (l'articolo 'un' viene sempre codificato con la chiave 're'). In questo caso il messaggio codificato conterrà pezzi di messaggio uguali, che consentirà a Chandisky di decrittare il messaggio.

Questo problema è collegato alla lunghezza della chiave. Per questo nasce il sistema di cifratura a *blocco monouso* (*one time pad*), in cui la chiave casuale è lunga quanto il testo da cifrare. È costituito da un'alta pila di fogli (pad). Ogni foglio è una chiave (usa e getta). È considerato il cifrario perfetto ma ha i seguenti limiti:

- la produzione di un numero elevato di chiavi casuali è molto oneroso
- la difficoltà di distribuzione e di protezione di tali chiavi ai destinatari

La sequenza casuale viene quindi sostituita da una sequenza *pseudocasuale*, in cui la chiave è composta da pochi caratteri, e la casualità è determinata dai pochi caratteri inseriti.

2.2 Algebra e Teoria dei numeri

Definizione 2.7. *Il* Principio di Kerkhoff *afferma che la sicurezza di un crittosistema deve basarsi non sul nascondere l'algoritmo di cifratura ma solo sul nascondere la chiave (ossia nel nascondere la quantità minima possibile di informazioni)*

Le cifrature possono essere a:

sostituzione sostituisce una lettera con un'altra lettera (cifrario di Cesare)

trasposizione traspone (sposta) le lettere dell'alfabeto

Esempio 2.4 Mostrare una possibile permutazione dell'insieme $A = \{1, 2, 3\}$

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Esempio 2.5 Crittare il testo "LACRITTOGRAFIAE'INTERESSANTE" utilizzando la tecnica della staccionata e scegliendo come chiave una matrice (2×14)

Il testo cifrato diventa:

```
LCITGAIEITRSATARTORFA'NEESNE
```

Infatti risulta:

```
LCITGAIEITRSAT
ARTORFA'NEESNE
```

che, letto colonna per colonna, restituisce il testo in chiaro

2.2.1 Cifratura a trasposizione

La trasposizione porta a determinare un maggior numero di chiavi, poiché se considero il numero di permutazioni in $\Sigma = 26$ ottengo 26! chiavi possibili.

Definizione 2.8. *Dato un insieme A finito e $|A| \equiv n$, si dice* permutazione *una qualunque applicazione biettiva di A in A*

Indicando con S_n l'insieme di tutte le permutazioni su n elementi, è dimostrabile che $|S_n| = n!$ Le permutazioni si indicano nel seguente modo:

$$f = \begin{pmatrix} 1 & \dots & n \\ f(1) & \dots & f(n) \end{pmatrix}$$

La più semplice tecnica di cifratura a traposizione è quella detta *staccionata* (*rail fenice*). Si scrive il testo in chiaro nelle colonne di una matrice e poi si legge il contenuto della riga giustapponendo il contenuto delle altre righe. Si veda l'esempio 2.5. Una variante consiste nell'eseguire i seguenti passi:

1. scegliere una matrice $(n \times m)$
2. scrivere il messaggio riga per riga
3. permutare l'ordine delle colonne
4. leggere il messaggio colonna per colonna

Si osservi a tale proposito l'esempio 2.6 Per rendere più sicuro il testo cifrato si può applicare più volte le permutazioni delle colonne, applicando il prodotto operatorio $f \circ f$ (o f^2)

Esempio 2.6 Crittare il testo "LACRITTOGRAFIAE'INTERESSANTE" utilizzando la variante della tecnica della staccionata e scegliendo come chiave una matrice (4×7)

Il testo in chiaro si trasforma nel seguente modo:

$$\begin{array}{ccccccc} L & A & C & R & I & T & T \\ O & G & R & A & F & I & A \\ E & ' & I & N & T & E & R \\ E & S & S & A & N & T & E \end{array}$$

Permuto le colonne:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 7 & 5 & 6 \end{pmatrix}$$

Da cui ottengo il testo cifrato:

`CRISRANAAG'SLOEETIETTAREIFTN`

Definizione 2.9. *Si definisce* prodotto operatorio *e si scrive $\varphi \circ \psi$ la permutazione che si ottiene applicando prima φ e poi ψ: $f \circ f : A \to A$ $f \circ f(x) : f(f(x))$*

Quindi si tratterà di applicare alla colonna 1: $(f \circ f)(1) = f(f(1)) = f(4) = 2$ e così via fino alla colonna finale.

2.3 Cifrario perfetto

Il cifrario perfetto segue il seguente schema:

1. viene costruita una chiave casuale lunga quanto il testo in chiaro e viene distribuita sia ad A che a B
2. per comunicare con B, A codifica addizionando mod 26 ogni lettera del testo in chiaro con una lettera della chiave. Poi distrugge la chiave.
3. B decodifica e poi distrugge la chiave

Attraverso la tabella *ASCII* (Amercian Standard Code for Information Interchange), è possibile trasformare l'alfabeto in binario. I caratteri ASCII sono composti da 7 bit, consentendo un numero di caratteri pari a 2^7. Per cifrare il testo basterà quindi eseguire uno XOR logico ($\oplus$) tra il testo in chiaro e la chiave generata.

2.4 Registri a scorrimento

Sono i generatori di sequenze pseudocasuali di bit. I vantaggi sono:

- possibile realizzare in hardware

Esempio 2.7 Calcolare i campi di Gaulois, sapendo che $m(x) = x^2 + x + 1$ e che $r(x) = ax + b$

Il numero di campi di Gaulois è $|\mathrm{GF}(2^2)| = 2^2 = 4$. I campi possibili sono:

a	b	$ax + b$
0	0	0
0	1	1
1	0	x
1	1	$x + 1$

da cui deriva che i 4 campi sono: $0, 1, x, x + 1$

- la matematica usata è quella dei campi finiti (o campi di Gaulois)

Definizione 2.10. *Un polinomio $f(x)$ di grado 2 si dice* irriducibile *se non può essere scritto come prodotto di due polinomi aventi grado almeno uno.*

I campi di Gaulois si scrivono con $\mathrm{GF}(2) = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. Sapendo che $m(x)$ rappresenta i polinomi e i coefficienti in $\mathbb{Z}_2$, con $m(x)$ irriducibile, si ha:

$$\mathrm{GF}(2^2) = \frac{\mathrm{GF}(2)[x]}{m(x)}$$

dove $m(x)$ sia un'equazione quadratica, tale quindi che il suo grado sia $\mathcal{O}(m) = 2$. Il grado del resto sarà chiaramente compreso tra i seguenti valori:

$$0 \leq \mathcal{O}r(x) \leq \mathcal{O}m(x)$$

Si veda l'esempio 2.7

2.4.1 Registri a scorrimento lineare

I *registri a scorrimento lineare* sono apparecchi elettronici capaci di moltiplicare e sommare polinomi a coefficienti in $\mathbb{Z}_2$ dal campo $\mathrm{GF}(2^n)$. I polinomi generati sono sequenze binarie. Sono composti da:

- n celle di memoria, collegate in serie, con un input e un output e capacità di un bit
- un clock, che invia periodicamente un segnale di scorrimento

A ogni segnale di scorrimento il contenuto di ogni cella passa nella cella successiva, secondo una funzione fissata chiamata *funzione di retroazione o di feedback*. I registri a scorrimento per loro natura hanno una relazione ben precisa tra stati interni e periodo della sequenza generata infatti, quando ritroviamo uno stato del registro uguale a quello iniziale, la sequenza degli output comincia a ripetersi. Allora il periodo di una sequenza pseudocasuale generata da un registro a scorrimento lineare è al più il numero massimo degli stati distinti, non nulli, del registro, cioè $2^n - 1$. Infatti, assunta la funzione di retroazione lineare, qualora all'interno del registro si vericasse lo

stato tutto nullo, il bit retroazionato sarebbe somma di bit nulli. In queste condizioni il registro a scorrimento assumerebbe sempre lo stato tutto nullo e quindi in uscita avremmo una sequenza tutta nulla da un certo bit in poi. Per tale motivo il polinomio di retroazione viene studiato in modo da escludere questa eventualità, riducendo il periodo massimo a $2^n - 1$.

2.5 Crittoanalisi

La crittoanalisi studia le strategie di attacco.

Definizione 2.11. *Un* protocollo *è una serie finita di operazioni tra due o più soggetti che utilizzano algoritmi crittografici per raggiungere un determinato scopo*

Definizione 2.12. *Un* attacco passivo *è un attacco in cui l'attaccante si inserisce sul canale di trasmissione (linea telefonica, etere, satellite, ...) e non fa altro che ascoltare e cercare di trarre informazioni*

Definizione 2.13. *Un* attacco attivo *è un attacco in cui l'attaccante cerca di alterare il protocollo a proprio vantaggio con inserimento di messaggi, alterazione di informazioni o contraffazione della propria identità.*

Gli attacchi possibili hanno la seguente classificazione, con riportati gli elementi che devono essere noti dall'attaccante per eseguire il particolare tipo di attacco:

Ciphertext-only necessari:

- algoritmo crittografico
- testo cifrato

Known-plaintext necessari:

- algoritmo crittografico
- testo cifrato
- una o più coppie testo in chiaro/testo cifrato generate con la chiave segreta

Chosen-plaintext necessari:

- algoritmo crittografico
- testo cifrato
- messaggio in chiaro scelto dal crittoanalista stesso assieme al corrispondente testo cifrato, generato con la chiave segreta

Chosen-ciphertext necessari:

- algoritmo crittografico
- testo cifrato

- testo cifrato scelto dall'attaccante assieme al corrispondente testo in chiaro decrittato, generato con la chiave segreta

Adaptative chosen-ciphertext (testo scelto) necessari:

- algoritmo crittografico
- testo cifrato
- messaggio in chiaro scelto assieme al corrispondente testo cifrato
- testo cifrato presunto scelto dall'attaccante assieme al testo in chiaro decrittato

Nella crittoanalisi si sfrutta il fatto che nel testo cifrato possono rimanere tracce indistinguibili della struttura o degli schemi del testo in chiaro. In particolare, l'*attacco a forza bruta* (anche detto per ricerca esaustiva) prova tutte le combinazioni su un frammento di testo cifrato. È riuscito a rompere nel 1998 il DES. In media per avere successo bisogna provare la metà di tutte le chiavi possibili. In seguito alla rottura fu ideato l'*AES* a 128 bit.

2.6 Metodi crittografici

I metodi crittografici classici hanno la seguente caratteristica: la cifratura e la decifratura hanno complessità computazionale uguale o dello stesso ordine. Si dice che sono computazionalmente equivalenti.

Definizione 2.14. *La* complessità computazionale *è il numero di operazioni elementari (operazioni svolte su una cifra binaria) eseguite dall'algoritmo*

Definizione 2.15. *Si dice* crittografica classica *(o* simmetrica *o* a chiave segreta*) la crittografia a cui appartengono i crittosistemi in cui, nota la chiave di cifratura, la funzione di decifratura f^{-1} può essere implementata con una complessità computazionale equivalente a quella della funzione di cifratura f*

Definizione 2.16. *Si dice* crittografia moderna *(o* asimmetrica *o* a chiave pubblica*) la crittografia a cui appartengono i crittosistemi in cui la funzione di decifratura f^{-1} presenta una complessità computazionale maggiore rispetto a quella di f*

Il problema della crittografia classica è lo scambio di chiavi. Se gli utenti sono n, e ognuno deve comunicare con ognuno, c'è bisogno di $\binom{n}{2}$ chiavi, ossia di $\frac{n(n-1)}{2}$ chiavi, ricordando che:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

2.7 Tipi di crittosistemi

I cifrari simmetrici si suddividono in:

Cifrari a flusso (Stream cipher) elaborano gli elementi di input in modo continuo un bit alla volta (o un byte) producendo l'output un elemento alla volta.

Ad esempio abbiamo il cifrario perfetto o i registri a scorrimento

Cifrari a blocchi (Block cipher) elaborano l'input in blocco di elementi per volta, ossia cifrano in sottoblocchi di lunghezza fissata l (cioè aventi lo stesso numero l di caratteri) e producono un blocco di output per ciascun blocco di input. l si dice *lunghezza del blocco*.

Ad esempio abbiamo:

- il Codice di Cesare con $l = 1$ e $\Sigma = \mathbb{Z}_{26}$. Tali cifrari sono un caso particolare e vengono chiamati *cifrari affini* o *cifrari a sostituzione*.
- il Codice di Vigenère in cui l è la lunghezza della parola chiave (ad es. tavola $l = 6$)

Proposizione 2.1. *Le trasformazioni crittografiche di un sistema a blocchi sono permutazioni*

2.7.1 Crittosistemi a blocchi

Un crittosistema a blocchi può avere differenti metodi di codifica:

ECB (Electronic Codebook Mode) aggiunge ad un messaggio di lunghezza arbitraria tanti caratteri casuali quanti sono necessari per ottenere un multiplo della lunghezza l del cifrario a blocchi usato. Poi si suddivide il testo in blocchi di lunghezza l, si cifrano uno per volta ed infine vengono concatenati.

CBC (Cipherblock Chaining Mode) è una variante di ECB in cui la codifica di un blocco dipende anche dai blocchi precedenti.

CFB (Cipher Feedback Mode) la funzione di cifratura genera blocchi di chiavi e non viene usata per la codifica del testo in chiaro. La cifratura viene ottenuta sommando mod 2 blocchi in chiaro con blocchi di chiave.

OFB (Output Feedback Mode) è una variante di CFB con velocità maggiore di trasmissione. Lo svantaggio è che la cifratura di un blocco non dipende anche dal blocco precedente.

2.8 DES (Data Encription Standard)

Il DES è un crittosistema di Feistel.

Definizione 2.17. *Si dice* crittosistema di Feistel *un sistema costruito sulla base di un cifrario a blocchi, di lunghezza l con alfabeto Σ e funzione di cifratura f_k dipendente da una chiave k.*

Un crittosistema di Feistel ha lunghezza del blocco $2l$, viene costruito in modo che per ogni fissata chiave k si generi una successione di sottochiavi $k_1, \ldots, k_r$ dette *chiavi di ciclo* o *di passo* che cifrano il blocco sottostante, con $r \geq 1$ (dove r rappresenta i rounds, ovvero la numerazione dei cicli). La funzione di cifratura F_k del crittosistema di Feistein è definita nel seguente modo:

1. si suddivide il testo in chiaro M di lunghezza $2l$ in due parti: L_0 (left) e R_0 (right) di eguale lunghezza l
$$M = (L_0, R_0)$$
2. si costruisce $\forall i\ 1 \leq i \leq r$ la successione
$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus f_{r_i}(R_{i-1})) \tag{2.1}$$
3. si opera ancora uno scambio tra destra e sinistra e si definisce
$$F_k(L_0, R_0) = (R_r, L_r)$$

Per definire la funzione di decifratura osserviamo dalla (2.1) che sarà ricavabile con:

$$(R_{i-1}, L_{i-1}) = (L_i, R_i \oplus f_{k_i}(L_i))$$

usando la sequenza inversa $k_r, \ldots, k_1$. Applicando la formula si ottiene quindi (L_0, R_0) a partire da (R_r, L_r). Si noti che non si parla di funzione inversa, poiché la F potrebbe non essere iniettiva.

Il sistema DES è un particolare sistema di Feistel avente lunghezza $2l = 64$, quindi $l = 32\,bit$ e numero di cicli (passi) $r = 16$. La funzione per crittare prevede 2 input: il testo in chiaro $2l = 64\,bit$ e la chiave di 56 bit, più 8 bit di controllo di parità. La differenza con il sistema di Feistel sta nel fatto che vengono inserite una permutazione iniziale π (IP) e una permutazione finale π^{-1} (FP). Quindi si avrà $\mathfrak{M} = \mathfrak{C} = \{0,1\}^{64}$, ma le chiavi sono blocchi di 56 bit più 8 bit di controllo. Il numero di chiavi sarà $2^{56} \cong 7 \cdot 10^{16}$ e schematicamente, dato il testo in chiaro r, si avrà:

$$\pi(r) \ldots \xrightarrow[\text{16 passi}]{\text{Crittosistema di Feistel}} \ldots \pi^{-1}(R_{16}, L_{16})$$

Lo schema è riportato anche in fig. 2.1 Nel 1998 il DES è stato rotto attraverso un attacco a forza bruta. In media per avere successo bisogna provare la metà di tutte le chiavi possibili. In seguito alla rottura fu ideato l'*AES* a 128 bit.

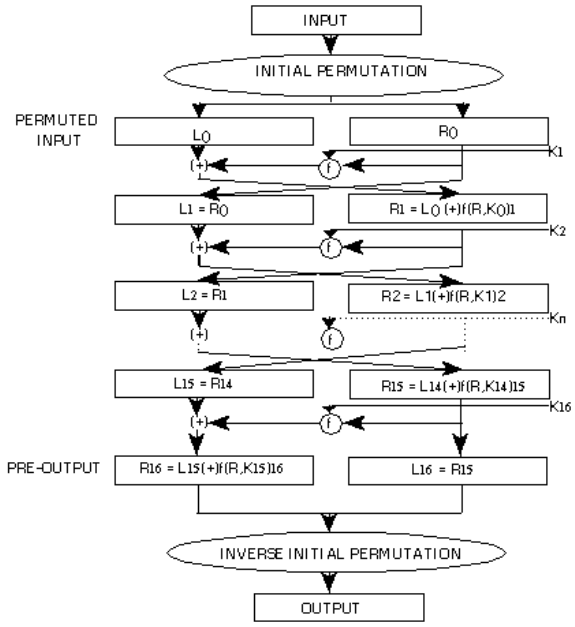

Figura 2.1: Lo schema del DES

3 Crittografia moderna (o a chiave pubblica)

3.1 Sicurezza Crittografica e Crittografia asimmetrica

La sicurezza di un sistema si classifica in:

Sicurezza computazionale se il miglior algoritmo noto che ne consente la violazione ha complessità computazionale superiore ad un certo limite N, sufficientemente grande.

Sicurezza dimostrabile se si riesce a fornire la prova che la sua sicurezza è equivalente a quella di un problema che si ritiene difficile da risolvere. La sicurezza non è assoluta ma relativa a quel sistema.

Sicurezza incondizionale se non è violabile neanche utilizzando una potenza di calcolo illimitata. La teoria di Shannon permette di studiare tale sicurezza (con la teoria della probabilità)

Teorema 3.1. Teorema di Shannon
La segretezza perfetta è possibile se e solo se l'insieme delle chiavi ha tanti elementi quanti ne ha l'insieme dei messaggi in chiaro. Nessuna chiave può essere utilizzata più di una volta (si consideri l'esempio del cifrario di Vernan).

Nel 1976 i due matematici Diffie ed Hellman pubblicarono un lavoro sullo scambio delle chiavi, in cui viene descritto un caso dove è indispensabile rendere nota la chiave pubblica. L'idea è:

- ogni utente sceglie una funzione crittografica f dipendente da alcuni parametri
- della funzione f saranno noti solo i parametri che permettono di cifrare i messaggi a lui diretti, utilizzando come chiave di codifica K_E (enciphering key)
- verrà mantenuta segreta invece la chiave di decodifica K_D (deciphering key).

Saranno rispettate due proprietà importanti:

- La funzione f può essere facilmente calcolabile conoscende K_E

$$f : \mathfrak{M} \to \mathfrak{C}$$

Esempio 3.1 Scomporre in fattori primi i seguenti numeri: 72, 123, 1763, 8633

72	2
36	2
18	2
9	3
3	3
1	

$$72 = 2^3 \cdot 3^2$$
$$123 = 3 \cdot 41$$
$$1763 = 41 \cdot 3$$
$$8633 = 89 \cdot 97$$

- La funzione f^{-1} tale che:
$$f^{-1} : f(\mathfrak{M}) \to \mathfrak{M}$$
non si può calcolare senza informazioni addizionali, ovvero senza conoscere K_D

Tali funzioni si dicono *unidirezionali* (*one way function* o *tradoor*).

Un esempio di funzioni unidirezionali viene dalla scomposizione di un numero in fattori primi, come si vede nell'es. 3.1.

Congettura 3.1. Congettura di Fermat

La congettura di Fermat afferma che

$$F_n = 2^{2^n} + 1$$

è primo per $1 \leq n \leq 4$*, mentre non vale per* $5 \leq n \leq 16$*. Nel 1990 è stato* dimostrato *che* F_9 *non è primo:*

$$F_9 = 2^{2^9} + 1 \cong 10^{45} + 1$$

che ha 513 bit e 155 cifre decimali.

Teorema 3.2. Teorema fondamentale dell'aritmetica

ogni numero naturale che non sia 1 ammette una ed una sola fattorizzazione in numeri primi non tenendo conto dell'ordine dei fattori. (L'esclusione di 1 è dovuta al fatto che esso non ha fattori primi.)

Dimostrazione. L'enunciato è facilmente verificabile per numeri naturali "piccoli": è facile scoprire che $70 = 2 \cdot 5 \cdot 7$ mentre $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 22 \cdot 52$, ed è altrettanto facile verificare che per questi numeri non possono esistere altre scomposizioni in fattori primi. Viceversa la dimostrazione generale è piuttosto lunga. Si tratta di una dimostrazione per assurdo che non mi sembra il caso di dimostrare ... □

Esempio 3.2 Calcolare se sussistono le seguenti congruenze: (1) $12 \equiv 6 \bmod 3$ (2) $18 \equiv 5 \bmod 3$ (3) $17 \equiv 23 \bmod 5$ (4) $45 \equiv 3 \bmod 7$

1. $12 = 6 \bmod 3$, poiché $\frac{12-6}{3} = 2$ con resto 0
2. $18 \neq 5 \bmod 3$, poiché $\frac{18-5}{3}$ non è divisibile
3. $17 = 23 \bmod 5$, poiché $\frac{17-23}{5} = 1$ con resto 0
4. $45 = 3 \bmod 7$, poiché $\frac{45-3}{7} = 6$ con resto 0

Esempio 3.3 Verificare la validità del teorema di Wilson per $n = 5$

$$\begin{aligned} (5-1)! &\equiv -1 \bmod 5 \\ 24 &\equiv 4 \bmod 5 \\ \frac{24-4}{5} &= 4 \quad \text{con resto } 0 \end{aligned}$$

Definizione 3.1. *Due numeri a e b si dicono* congrui modulo n *e si esprime $a \equiv b \bmod n$ se esiste un intero k per cui*

$$\begin{aligned} a - b &= k \cdot n \\ a &= k \cdot n + b \end{aligned}$$

cioè se a e b divisi per n danno lo stesso resto.

Si veda l'es. 3.2

Esiste una condizione necessaria e sufficiente che consente di stabilire se un intero $n \leq 2$ è un numero primo, nota come il *Teorema di Wilson*.

Teorema 3.3. Teorema di Wilson
dato un numero primo $n > 1$,

$$(n-1)! \equiv -1 \bmod n$$

La condizione del Teorema di Wilson è riscrivibile come:

$$\begin{aligned} (n-1)! &\equiv -1 \bmod n \\ (n-1)! + 1 &\equiv 0 \bmod n \\ (n-1)! + 1 &\equiv K_n \quad K \in \mathbb{Z} \end{aligned}$$

Si osservi per il Teorema di Wilson l'es. 3.3 e l'es. 3.4

Esempio 3.4 Verificare la validità del teorema di Wilson per $n = 6$

$$
\begin{aligned}
(6-1)! &\equiv -1 \bmod 6 \\
5! = 5 \cdot 4 \cdot 3 \cdot 2 = 20 \cdot 6 &=_6 2 \cdot 0 = 0 \\
0 &\neq 5 \bmod 6 \\
\frac{0-5}{6} &\quad \text{non divisibile}
\end{aligned}
$$

Esempio 3.5 Verificare la validità del teorema di Fermat per $n = 15$

$$a^{15} \cong a \bmod 15 \qquad a \in [1, 14]$$

$$
\begin{array}{llll}
1^{15} \equiv_{15} 1 & 2^{15} \equiv_{15} 8 & 3^{15} \equiv_{15} 12 & 4^{15} \equiv_{15} 4 \\
5^{15} \equiv_{15} 5 & 6^{15} \equiv_{15} 6 & 7^{15} \equiv_{15} 13 & 8^{15} \equiv_{15} 2 \\
9^{15} \equiv_{15} 9 & 10^{15} \equiv_{15} 10 & 11^{15} \equiv_{15} 11 & 12^{15} \equiv_{15} 3 \\
13^{15} \equiv_{15} 7 & 14^{15} \equiv_{15} 14 &&
\end{array}
$$

Teorema 3.4. Teorema di Fermat
Sia p un numero primo. Risulta:

$$\forall a \in \mathbb{Z}\ t.c\ 1 \leq a \leq p-1 \Rightarrow (a, p) = 1$$

indicando con (a, p) il massimo comun divisore tra a e p. Quanto affermato può essere riscritto come segue:

$$
\begin{aligned}
a^{p-1} &\equiv 1 \bmod p \\
a^{p} &\equiv a \bmod p \\
a^{p-2} &\equiv a^{-1} \bmod p
\end{aligned}
$$

In altre parole, se p è un numero primo, allora $\forall a \in [1, p-1]$ abbiamo classi di congruenza distinte.

Si veda l'es. 3.5 per un'applicazione del teorema di Fermat. Se un numero n rispetta le condizioni del teorema di Fermat, si deduce che sia *molto probabile* che sia un numero primo. Un intero non primo che rispetta le condizioni del teorema di Fermat per una particolare base è chiamato numero *pseudoprimo.*

Definizione 3.2. *Si dice che $n \in \mathbb{Z}$ è un numero* pseudoprimo *in base $a \in \mathbb{N}^*$ (cioè tranne lo 0) se n:*

Esempio 3.6 Determinare il più piccolo pseudoprimo sulla base 2

Il numero è 341. Infatti rispetta le due condizioni:

- $341 = 11 \cdot 31$
- $2^{340} \equiv 1 \bmod 341$

Si noti che non risulta probabilmente primo sulla base 3:

$$3^{340} \neq 1 \bmod 341$$

- *è un numero composto*
- *rispetta la condizione di Fermat:* $a^{n-1} \equiv 1 \bmod n$

Si veda l'es. 3.5

Definizione 3.3. *Gli interi n si dicono* numeri di Carmichael *se sono pseudoprimi* $\forall a$ *t.c.* $(a, n) = 1$

Per determinare i numeri di Carmichael è necessaria la conoscenza del teorema cinese del resto:

Teorema 3.5. *Teorema Cinese del Resto*
Il sistema di congruenze:

$$\begin{cases} x = a \bmod n \\ x = b \bmod m \end{cases}$$

ha soluzione se e solo se

$$a = b \bmod (\mathrm{mcd}(n, m))$$

Si veda l'es. 3.7 per vedere l'applicazione del teorema cinese del resto nella determinazione dei numeri di carmichael.

3.2 Logaritmo discreto

Il logaritmo discreto si basa sulla teoria dei gruppi.

Definizione 3.4. *Un* gruppo *è una struttura composta da:*

- *un insieme A*
- *una operazione binaria op che soddisfa alcuni assiomi descritti*

Il gruppo verrà identificato con (A, op)

Definizione 3.5. *Un* gruppo abeliano*, o* gruppo commutativo*, è un gruppo la cui operazione binaria gode della proprietà commutativa*

Esempio 3.7 Mostrare che $n = 561$ è un numero di Carmichael

Innanzitutto si osserva che 561 non è primo:

$$561 = 3 \cdot 11 \cdot 17$$

Affinché sia un numero di Carmichael, è necessario $\forall a$ t.c. $(a, n) = 1$ sia verificata la condizione di Fermat. Nel nostro caso $a = 3$, $a = 11$, $a = 17$.

$$\begin{cases} a^2 & \equiv 1 \bmod 3 \\ a^{10} & \equiv 1 \bmod 11 \\ a^{16} & \equiv 1 \bmod 17 \end{cases}$$

Da cui si ricava: $\text{mcm}(2, 10, 16) = 80$ e $\text{mcd}(3, 11, 17) = 561$. Le tre congruenze sono equivalenti alla seguente:

$$\begin{aligned} a^{80} &\equiv 1 \bmod 561 \\ (a^{80})^7 &\equiv (1 \bmod 561)^7 \\ a^{560} &\equiv 1^7 \bmod 561 \\ a^{560} &\equiv 1 \bmod 561 \\ a^{n-1} &\equiv 1 \bmod n \end{aligned}$$

Quindi $n = 561$ è un numero di Carmichael.

Esempio 3.8 Verificare se $a = 4$ è un generatore di $\mathbb{Z}_{11}^*$. Riportare l'ordine di a

$4^0 =_{11} 1$ $\quad$ $4^1 =_{11} 4$

$4^2 =_{11} 5$ $\quad$ $4^3 = 4^2 \cdot 4 = 20 =_{11} 9$

$4^4 = 4^2 \cdot 4^2 = 5 \cdot 5 = 25 =_{11} 3$ $\quad$ $4^5 = 4^4 \cdot 4 = 3 \cdot 4 = 12 =_{11} \boxed{1}$

$4^6 = 4^5 \cdot 4 = 1 \cdot 4 = 4 =_{11} \boxed{4}$ $\quad$ .....

L'ordine di $a = 4$ è 5, poiché è il primo numero positivo da cui ricomincia il ciclo.

Ad esempio, il gruppo $(\mathbb{Z}_m, +)$ forma un gruppo. In particolare il gruppo gode delle seguenti proprietà:

- somma commutativa
- somma associativa: $\overline{a} + \overline{b} =_m \overline{a+b}$
- esiste l'elemento neutro $\overline{0}$
- ogni elemento ha il suo opposto: $\overline{a} + (-\overline{a}) = \overline{0}$

Quindi questo gruppo è anche abeliano. Anche il gruppo $(\mathbb{Z}_m, \cdot)$ forma un gruppo, poiché sono verificate le seguenti proprietà:

- moltiplicazione commutativa
- moltiplicazione associativa
- esiste l'elemento neutro $\overline{1}$
- ogni elemento $\neq \overline{0}$ ha il suo opposto: $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$

Definizione 3.6. *Un* gruppo ciclico *è un gruppo che può essere generato da un solo elemento, cioè esiste un elemento g del gruppo (detto* generatore*) tale che ogni altro elemento si ottiene componendo n volte g con se stesso (tale operazione si scrive g^n)*

Quindi, dato il gruppo $(\mathbb{Z}_{11}, \cdot)$, si scrive $< g >= \mathbb{Z}_{11}^*$. Dato che il numero di classi di equivalenza saranno pari a $|\mathbb{Z}_{11}^*| = 10$, risulta $\mathbb{Z}_{11} = \{g^0, \ldots, g^9\}$

Definizione 3.7. *L'*ordine *di un elemento $a \in G$ è il minimo intero positivo $\mathcal{O}$ per cui $a^{\mathcal{O}} = 1$ (cioè il primo elemento in cui il ciclo ricomincia).*

Si vedano gli esempi 3.8 e 3.9 Per calcolare quanti sono i possibili generatori si utilizza la funzione di Eulero.

Definizione 3.8. *La* funzione di Eulero *esprime l'ordine dell'insieme:*

$$\varphi(m) = |\{x | x < m, (x, m) = 1\}|$$

Esempio 3.9 Verificare se $a = 7$ è un generatore di $\mathbb{Z}_{11}^*$. Riportare l'ordine di a

$$7^0 =_{11} 1 \qquad 7^1 =_{11} 7$$
$$7^2 =_{11} 5 \qquad 7^3 = 7^2 \cdot 7 = 5 \cdot 7 = 35 =_{11} 2$$
$$7^4 = 7^2 \cdot 7^2 = 5 \cdot 5 = 25 =_{11} 3 \qquad 7^5 = 7^3 \cdot 7^2 = 2 \cdot 5 = 10 =_{11} 10$$
$$7^6 = 7^4 \cdot 7^2 = 3 \cdot 5 = 15 =_{11} 4 \qquad 7^7 = 7^4 \cdot 7^3 = 3 \cdot 2 = 6 =_{11} 6$$
$$7^8 = 7^4 \cdot 7^4 = 3 \cdot 3 = 9 =_{11} 9 \qquad 7^9 = 7^6 \cdot 7^3 = 4 \cdot 2 = 8 =_{11} 8$$
$$7^{10} = 7^4 \cdot 7^6 = 3 \cdot 4 = 12 =_{11}$$

Osserviamo che $a = 7$ copre 10 elementi (da 7^0 a 7^9). Perciò $a = 7$ è un generatore e possiamo scrivere $\mathbb{Z}_{11}^* =< 7 >$. L'ordine di $a = 5$ è 10.

Esempio 3.10 Calcolare quanti sono i generatori per $\mathbb{Z}_{11}^*$ e per $\mathbb{Z}_{12}^*$

Per $\mathbb{Z}_{11}^*$ si determineranno gli $x < 10$ tali che $(x, 10) = 1$:

$$\varphi(10) = |\{1, 3, 7, 9\}| = 4$$

Per $\mathbb{Z}_{12}^*$ si determineranno gli $x < 11$ tali che $(x, 11) = 1$. Ma si nota che 11 è un numero primo, quindi vale immediatamente:

$$\varphi(11) = 10$$

Infatti tutti gli $x < 11$ avranno $(x, 11) = 1$.

Quindi $\varphi(m)$ indica quanti sono i g tali che $< g >= \mathbb{Z}_p^*$.

Proposizione 3.1. *Per un qualunque m, i generatori di $\mathbb{Z}_m^*$ sono in numero $\varphi(m-1)$*

Proposizione 3.2. *Per ogni numero primo p, $\varphi(p) = p - 1$*

Si veda l'es. 3.10. Ma se vogliamo determinare *quali* siano i generatori vale la seguente proposizione:

Proposizione 3.3. *Se α è un generatore, tutti i generatori di $\mathbb{Z}_m^*$ sono tutti gli*

$$\alpha^h \qquad \forall h < m - 1 \Rightarrow (h, m - 1) = 1$$

Si veda l'es. 3.11

Definizione 3.9. *Gli* elementi invertibili *in $\mathbb{Z}_m^*$ sono tutti gli $a \in \mathbb{Z}$ tali che $(a, m) = 1$*

Ad esempio, il gruppo $(\mathbb{Z}_4, \cdot)$ avrà lo schema riportato in tab. 3.1, dove si nota che l'elemento $\overline{2}$ non è invertibile. Si noti che in $\mathbb{Z}_{11}$ tutti gli elementi sono invertibili.

Esempio 3.11 Determinare quali sono tutti i possibili generatori di $\mathbb{Z}_{11}$, sapendo che $\varphi(10) = 4$ e che un generatore vale $g = 7$

Per $\mathbb{Z}_{11}^*$ si determineranno gli $h < 10$ tali che $(h, 10) = 1$. I valori ricavati $\{1, 3, 7, 9\}$ sono utilizzati per ricavare i rimanenti 3 generatori:

$$7^1 =_{11} 7 \qquad 7^3 =_{11} 2 \qquad 7^7 =_{11} 6 \qquad 7^9 =_{11} 8$$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	0	0	0	0
$\overline{1}$	0	1	2	3
$\overline{2}$	0	2	0	2
$\overline{3}$	0	3	2	1

Tabella 3.1: Schema del gruppo $(\mathbb{Z}_4, \cdot)$

Se si considerano tutti i possibili generatori, qual è la relazione tra di loro? In $\mathbb{Z}_{11}^*$ con generatori 7, 2, 6 e 8 si verifica:

$$7 \cdot 8 = 56 = 55 + 1 =_{11} 1 \qquad 2 \cdot 6 = 12 = 11 + 1 =_{11} 1$$
$$7 \cdot 6 = 42 \neq_{11} 1 \qquad 2 \cdot 8 \neq_{11} 1$$
$$7 \cdot 2 = 14 \neq_{11} 1$$

Da cui si ricava che 7 e 8, e 2 e 6 sono l'uno l'inverso dell'altra:

$$7 = 8^{-1} \qquad 8 = 7^{-1} \qquad 2 = 6^{-1} \qquad 6 = 2^{-1}$$

3.3 Schema dello scambio delle chiavi (Diffie–Hellmann)

L'*esempio dei lucchetti* illustra il seguente procedimento per impedire l'accesso alle chiavi.

1. A spedisce un pacco con un messaggio a B chiuso con il lucchetto L_A
2. B riceve il pacco chiuso con L_A. Aggiunge L_B e rispedisce il pacco ad A
3. A toglie L_A e rispedisce il pacco a B
4. B toglie L_B e legge il messaggio

Lo schema dello scambio delle chiavi è basato sull'utilizzo di una funzione unidirezionale. Dato un numero primo p e un generatore g si avrà:

$$f : x \to g^x \bmod p$$
$$f^{-1} : y \to x = \log_g y \bmod p$$

Lo schema diventa di scambio delle chiavi è riportato in tab. 3.2

A	**B**
A sceglie un elemento di $\mathbb{Z}_{10}$ ossia sceglie $a \in \{0, \ldots, 9\}$ con $a \neq 0$ e $a \neq 1$. Sceglie $a = 3$	B sceglie $b \in \mathbb{Z}_{10}$ tale che $b \neq 0$ e $b \neq 1$. Sceglie $b = 6$.
A computa $g^a = 7^3 \bmod 11 = 2$	B computa $g^b = 7^6 \bmod 11 = 4$
A trasmette a B $g^a = 2$	B trasmette ad A $g^b = 4$
Nota: 2 e 4 non sono le chiavi segrete. Le chiavi segrete sono $a = 3$ e $b = 4$	
A, usando il risultato ricevuto da B, computa: $(g^b)^a = (4)^3 =_{11} 9$	B computa: $(g^a)^b = (2)^6 =_{11} 9$
La chiave pubblica è $g^{ab} = 9$, la chiave privata di a e di b consentono di decifrare	

Tabella 3.2: Schema Diffie–Hellmann di scambio delle chiavi in $\mathbb{Z}_{11}$ con $p = 11$ e $g = 7$

3.4 RSA (Rivest–Shamir–Adleman)

RSA è il più noto sistema a chiave pubblica che permette di ottenere:

- riservatezza
- integrità
- autenticazione

Ogni utente A compie le seguenti operazioni una sola volta:

1. sceglie 2 numeri primi p e q distinti e molto grandi
2. calcola
$$n = p - q$$
3. calcola
$$\varphi(n) = \varphi(p - q) = \varphi(p) \cdot \varphi(q) = (p - 1) \cdot (q - 1)$$
4. sceglie $e < n$ tale che e e n siano coprimi tra loro, ovvero tale che
$$(e, \varphi(n)) = 1$$
Si noti che $\varphi(n)$ in quanto prodotto di due numeri $(p - 1) \cdot (q - 1)$, sarà pari. Quindi e sarà necessariamente dispari.
5. determina $d \in \mathbb{Z}^*_{\varphi(n)}$ tale che
$$\begin{aligned} e \cdot d &\equiv 1 \bmod \varphi(n) \\ d &\equiv e^{-1} \bmod \varphi(n) \end{aligned}$$
6. rende nota la coppia $\{n, e\}$ che è la sua *chiave pubblica*
7. tiene segreti p, q, d che costituiscono la sua *chiave privata*

La *funzione crittografica* di A (ovvero l'algoritmo crittograrfico) è:

$$\begin{aligned} f_A(m) &= m^e \bmod n \\ e &= m^e \bmod n \\ f_A^{-1}(c) &= c^d \bmod n \\ c^d \bmod n &= (m^e)^d \bmod n = m \bmod n \end{aligned}$$

Nel 2004 i laboratori RSA consigliavano come minimo:

- n di lunghezza almeno 1024 bit ($\sim$ 308 cifre decimali) per la non violazione entro il 2010
- n di lunghezza 2048 bit ($\sim$ 616 cifre decimali) per la non violazione entro il 2030

3.4.1 Esempio generazione chiavi

L'esempio seguente mostra in particolare come risolvere la congruenza lineare $e \cdot d \equiv 1 \bmod \varphi(n)$. I passi sono i seguenti:

1. *A* sceglie $p = 17$ e $q = 11$
2. calcola $n = p \cdot q = 187$
3. calcola $\varphi(n) = (p-1) \cdot (q-1) = 16 \cdot 10 = 160$
4. sceglie $e < n$ tale che $(e, \varphi(n)) = 1$. Si sceglie $e = 7$, poiché $7 < 187$ e $(7, 160) = 1$. Sono quindi coprimi tra loro
5. calcola $d \in \mathbb{Z}^*_{\varphi(n)}$ tale che $e \cdot d \equiv 1 \bmod \varphi(n)$ (oppure $d \equiv e^{-1} \bmod \varphi(n)$)

   Il Teorema di Eulero esamina iterativamente tutte le possibilità:

   $$(a, r) = 1 \Rightarrow a^{\varphi(r)} = 1 \bmod r, \quad a^{\varphi(r)-1} = a^{-1} \bmod r, \quad \ldots$$

   Ma è un procedimento troppo lungo poiché n in pratica è troppo grande (e quindi lo sarà anche $r = \varphi(n)$).

   La soluzione è applicare le congruenze lineari. Calcoliamo d risolvendo la seguente congruenza lineare nell'incognita $x = d$:

   $$\begin{aligned} e \cdot d &\equiv 1 \bmod \varphi(n) \\ ax &\equiv b \bmod m \end{aligned}$$

   Se la congruenza ammette soluzioni:

   $$(a, m) = k$$

   allora avremo soddisfatta la condizione k/b, ovvero k divide b e la congruenza ammette soluzioni.

   Nel nostro caso, avremo:

   $$\begin{aligned} 7x &\equiv 1 \bmod 160 \\ (7, 160) &= 1 \end{aligned}$$

   poiché nel nostro caso $b = 1$ allora avremo soddisfatta la condizione $1/1$ e la congruenza ammette soluzioni. Per risolvere la congruenza è necessario riuscire a scrivere l'espressione:

   $$1 = h_1 160 + h_2 7$$

   Si applica a tale scopo l'*algoritmo di Euclide* (o algoritmo delle divisioni successive) di m per a

160	7
7	6
6	1

   $$\begin{aligned} 160 &= 7 \cdot 22 + 6 \\ 7 &= 6 \cdot 1 + \boxed{1} \longleftarrow \text{mcd}(160, 7) \\ 6 &= 1 \cdot 6 + \boxed{0} \longleftarrow \text{mi fermo} \end{aligned}$$

Esprimo le equazioni in funzione del resto ottenuto:

$$\begin{cases} 6 = 160 + 7(-22) \\ 1 = 7 + 6(-1) \end{cases}$$

Da cui si ricava sostituendo tra di loro le equazioni:

$$\begin{aligned} 1 &= 7 + 6(-1) \\ &= 7 + (160 + 7(-22))(-1) \\ &= 7 + 160(-1) + 7(22) \\ &= 7(23) + 160(-1) \\ &= (-1) \cdot 160 + 23 \cdot 7 \\ &= h_1 160 + h_2 7 \end{aligned}$$

Allora la risoluzione della congruenze sarà:

$$\begin{aligned} 7x &\equiv 1 \bmod 160 \\ 7x - 1 &= 160z' \qquad z' \in \mathbb{Z} \\ 7x + 160(-z') &= 1 \\ 7x + 160(z) &= 1 \qquad z = -z' \end{aligned}$$

Allora la soluzione è $x = h_2$, quindi $x = 23$. Riportato quindi nel "dominio delle congruenze", risulta $x = [23]_{160}$.

Risulta quindi che il $d \in \mathbb{Z}^*_{\varphi(n)}$ tale che $e \cdot d \equiv 1 \bmod \varphi(n)$ vale $d = 23$

6. rende nota la coppia $\{n, e\}$, quindi $K_P(187, 7)$, che è la sua chiave pubblica
7. tiene segreti p, q, d, quindi $K_S(17, 11, 23)$ che costituiscono la sua chiave privata

3.4.2 Esempio applicazione funzione crittografica

Il prossimo esempio illustra come applicare la funzione crittografica. B vuole inviare ad A il messaggio "vado!". I codici ASCII corrispondenti sono $v = 22$, $a = 01$, $d = 04$, $o = 15$, $! = 28$. Vengono scelti $p = 5$ e $q = 11$.

1. $p = 5$ e $q = 11$
2. $n = p \cdot q = 5 \cdot 11 = 55$
3. $\varphi(n) = (p - 1) \cdot (q - 1) = 4 \cdot 10 = 40$
4. scelgo $e < 55$ tale che $(e, 40) = 1$. Si pone $e = 3$
5. determino $x = d$ tale che $3x \cong 1 \bmod 40$. Risulta $d = 27$.
6. rendo nota la chiave pubblica $K_P(55, 3)$

7. tengo segreta la chiave privata $K_S(5, 11, 27)$

Il messaggio m risulta:

$$m = \underbrace{22}_{m_1}\ \underbrace{01}_{m_2}\ \underbrace{04}_{m_3}\ \underbrace{15}_{m_4}\ \underbrace{28}_{m_5}$$

Dove i sottoblocchi sono stati suddivisi con una lunghezza $k = 2$. Una lunghezza $k = 3$ non sarebbe stata possibile poiché deve essere rispettata la condizionata che n deve essere $\geq$ dei codici ASCII risultanti. Nel caso $k = 3$ sarebbe risultato $220 \not< 55$. Applicando $k = 2$ si verifica invece $22 < 55$.

Applicando la funzione crittografica $c = m^e \bmod n$ risulta:

$$\begin{aligned}
c_1 = m_1^e \bmod n &= 22^3 \bmod 55 = 33 \\
c_2 = m_2^e \bmod n &= 01^3 \bmod 55 = 01 \\
c_3 = m_3^e \bmod n &= 04^3 \bmod 55 = 09 \\
c_4 = m_4^e \bmod n &= 15^3 \bmod 55 = 20 \\
c_5 = m_5^e \bmod n &= 28^3 \bmod 55 = 07
\end{aligned}$$

Da cui deriva che il messaggio codificato c risulta:

$$m = \underbrace{33}_{c_1}\ \underbrace{01}_{c_2}\ \underbrace{09}_{c_3}\ \underbrace{20}_{c_4}\ \underbrace{07}_{c_5}$$

Per decrittare si userà la funzione $m = c^d \bmod n$:

$$\begin{aligned}
m_1 = c_1^d \bmod n &= 33^{27} \bmod 55 = 22 \\
m_2 = c_2^d \bmod n &= 01^{27} \bmod 55 = 01 \\
m_3 = c_3^d \bmod n &= 09^{27} \bmod 55 = 04 \\
m_4 = c_4^d \bmod n &= 20^{27} \bmod 55 = 15 \\
m_5 = c_5^d \bmod n &= 07^{27} \bmod 55 = 28
\end{aligned}$$

Da cui si ricostruirà il messaggio "vado!" originario.

3.4.3 Esempio in binario

Riprendendo l'esempio precedente traduciamo col codice ASCII *in binario* il messaggio "vado!" risulta:

$$m = \underbrace{01010110}_{\text{'v'}}\underbrace{01000001}_{\text{'a'}}\underbrace{01000100}_{\text{'d'}}\underbrace{01001111}_{\text{'o'}}\underbrace{00100000}_{\text{'!'}}$$

Risultava $n = 55$, quindi in binario $n = 110111$, che ha lunghezza 6 bit. I sottoblocchi devono quindi avere lunghezza $k < 6$[1]. Scelgo $k = 5$. Quindi avrò:

$$m = \underbrace{01010}_{10}\underbrace{110\quad 01}_{25\quad\ 0}\underbrace{00001}_{\ 20}\underbrace{0\quad 0100}_{\ 8}\underbrace{0100\quad 0}_{19\quad\ 25}\underbrace{1001111}_{\ 0}\underbrace{001\quad 00000}_{\ 0}$$

[1] Scegliere un k minore al numero di bit è forse una restrizione eccessiva, in quanto se ho $n = 111111$ non ho bisogno di scegliere $k < 6$ per soddisfare la condizione

Il messaggio m sarà quindi:

$$m = \underbrace{10}_{c_1}\underbrace{25}_{c_2}\underbrace{0}_{c_3}\underbrace{20}_{c_4}\underbrace{8}_{c_5}\underbrace{19}_{c_6}\underbrace{25}_{c_7}\underbrace{0}_{c_8}$$

Applicando la funzione crittografica $c = m^e \bmod n$, sapendo che la chiave pubblica risulta $e = 3$, risulta:

$$\begin{aligned}
c_1 &= m_1^e \bmod n & &= 10^3 \bmod 55 = 10 \\
c_2 &= m_2^e \bmod n & &= 25^3 \bmod 55 = 5 \\
c_3 &= m_3^e \bmod n & &= 0^3 \bmod 55 = 0 \\
c_4 &= m_4^e \bmod n & &= 20^3 \bmod 55 = 25 \\
c_5 &= m_5^e \bmod n & &= 8^3 \bmod 55 = 17 \\
c_6 &= m_6^e \bmod n & &= 19^3 \bmod 55 = 39 \\
c_7 &= m_7^e \bmod n & &= 25^3 \bmod 55 = 5 \\
c_8 &= m_8^e \bmod n & &= 0^3 \bmod 55 = 0
\end{aligned}$$

B trasmette in binario:

$$c = \underbrace{1010}_{10}\underbrace{101}_{5}\underbrace{0}_{0}\underbrace{11001}_{25}\underbrace{10001}_{17}\underbrace{100111}_{39}\underbrace{101}_{5}\underbrace{0}_{0}$$

A riceve, converte in decimale la sequenza e decritta utilizzando la funzione $m = c^d \bmod n$. Applica il metodo e ritrasmette in binario prendendo sottoblocchi di un byte:

$$m = \underbrace{01010}_{\text{'v'}}\underbrace{110}\underbrace{01}\underbrace{00000}_{\text{'a'}}\underbrace{1}\underbrace{0100}\underbrace{0100}_{\text{'d'}}\underbrace{0}\underbrace{10011}_{\text{'o'}}\underbrace{11}\underbrace{001}\underbrace{00000}_{\text{'!'}}$$

3.4.4 Attacchi all'RSA

L'RSA ha alcuni punti critici:

- lentezza di codifica: calcolare $\varphi(n)$ è computazionalmente equivalente a calcolare p e q
- la scelta di p e q deve dar luogo a cosiddetti *primi forti*:
  1. n non deve avere fattori primi piccoli
  2. n non deve avere fattori tra loro vicini
  3. n non deve avere la proprietà che $n+1$ o $n-1$ siano formati da primi piccoli

Gli attacchi possibili sono riportati di seguito.

Testo cifrato scelto

Sia A un utente con chiave pubblica $K_P = (n, e)$, che ottiene un messaggio cifrato c, $c = m^e \bmod n$. L'intruso sceglie un intero r, computa $c^1 = r^e \cdot c$ e chiede ad A di decifrare c' con la chiave *segreta* di A. A non sa che in realtà c' è legato a c. Se A esegue, l'intruso ottiene la decodifica di c^1 e alla fine riesce a descrittare m.

Quindi, sia m' la decodifica di c': $m' = c'^d \bmod n$. Allora

$$\begin{aligned} m' &= c'^d \\ &= (r^e \cdot c)^d \\ &= r^{ed} \cdot c^d \\ r^{-1}m' &= c^d \\ m &= c^d \qquad \text{per ipotesi} \\ r^{-1}m' &= m \end{aligned}$$

Quindi l'intruso legge m senza conoscere d. A non deve quindi decifrare messaggi di cui non è sicuro. È quindi opportuno utilizzare una funzione hash e autenticare.

Attacco elementare

Bisogna evitare una scelta del $\bmod(n)$ fissata per tutti gli utenti. Infatti se B conosce che A ha $n_A = n_B$, può calcolare $\varphi(n)$ e risalire a $d_A = e_A^{-1} \bmod \varphi(n)$. L'intruso, da due codifiche c_1 e c_2 di un messaggio m, ricavate da due chiavi pubbliche (n, e_1) ed (n, e_2) con $(e_1, e_2) = 1$, può ricavare il messaggio in chiaro m come segue:

1. conosce n, e_1, e_2, c_1 e c_2. Allora:

$$(e_1, e_2) = 1 \Rightarrow 1 = re_1 + se_1 \qquad r, s \in \mathbb{Z}$$

2. calcola:

$$\begin{aligned} m &= m' \\ &= m^{re_1 + se_2} \\ &= (m^{e_1})^r \cdot (m^{e_2})^s \\ &= c_1^r \cdot c_2^s \bmod n \qquad \text{poiché } c_1 = m^{e_1} \bmod n \end{aligned}$$

3. parte da c_1^r e c_2^s ed ottiene m

$$c_1 \cdot c_1^{-1} \equiv 1 \bmod n.$$

$$r \Rightarrow \begin{cases} (c_1)^{-r} & r \geq 0 \\ (c_1^{-1})^{-r} & r < 0 \end{cases}$$

In conclusione, ogni n non deve essere usato per più di un utente.

3.4.5 Firma digitale (o elettronica) con RSA

La *firma digitale* serve per autenticare una qualunque sequenza di bit, indipendentemente dal loro significato. Nella crittografia a chiave pubblica abbiamo due utenti A e B con rispettivamente funzione di cifratura f_A e f_B e funzione di decifratura f_A^{-1} e f_B^{-1}. Tali funzioni sono messe a disposizione dall'*Ente Certificatore*

A vuole inviare il messaggio m a B e firmare elettronicamente. La firma digitale di A sarà indicata con $f_A^{-1}(s_A)$, dove s_A è un nome convenzionale di A che contiene:

- un numero progressivo
- un'indicazione del tempo in cui è stato spedito m

Quindi A invia, oltre al messaggio cifrato c con (ad esempio) RSA, $f_B(f_A^{-1}(s_A))$. La codifica con f_A^{-1} garantisce l'*autenticazione* di A, mentre la codifica con f_B garantisce la *riservatezza*, in quanto solo B sarà in grado di decifrare il messaggio.

B decifra c e verifica se la firma è proprio di A, applicando il prodotto operatorio come segue:

$$\begin{aligned}(f_A \circ f_B^{-1})(f_B(f_A^{-1}(s_A)) \\ f_A(f_B^{-1}(f_B(f_A^{-1}(s_A)))) \\ f_A(f_A^{-1}(s_A)) \\ s_A\end{aligned}$$

In questo modo, oltre a riservatezza ed autenticazione viene garantita la terza importante proprietà: l'*integrità*.

Per rendere più sicuro questo processo si può far dipendere la firma digitale dal messaggio stesso. Quindi la firma diventa $f^{-1}(h(m))$ con h funzione hash e $h(m)$ impronta di m tramite h.

Definizione 3.10. *sia Σ l'alfabeto, Σ^n l'insieme di tutte le n-ple (parole o stringhe di lunghezza n), allora*

$$\Sigma^* = \bigcup_{i=1}^{\infty} \Sigma^i$$

si dice funzione hash *un'applicazione:*

$$h : \Sigma^* \to \Sigma^n \qquad n \in \mathbb{N}$$

che ad una parola di lunghezza arbitraria associa una parola di lunghezza fissata.

Le funzioni hash utilizzate in pratica sono pubbliche e disponibili a tutti gli utenti. Ne viene utilizzata una sola per tutti gli utenti di un sistema.

Definizione 3.11. *Si dice* collisione della funzione hash h *una coppia $(a, b) \in \Sigma^* \times \Sigma^*$, $a \neq b$ tale che $h(a) = h(b)$ (hanno quindi la stessa immagine)*

Ricapitolando lo schema con l'ausilio della funzione hash, A codifica il messaggio in chiaro m e firma il messaggio cifrato c con $f_A^{-1}(h(m))$ dove $h(m)$, impronta di h ha di solito 160 cifre binarie. A invia quindi a B:

- il messaggio codificato c
- la firma $f_B(f_A^{-1}(h(m)))$, codificata anche con f_B per garantirne la riservatezza

3.5 Crittosistema di Rabin

Il *crittosistema di Rabin* è un altro sistema che si basa sulla fattorizzazione di interi. Lo schema è il seguente:

1. A sceglie due numeri primi $p \equiv 3 \bmod 4$ e $q \equiv 3 \bmod 4$. Calcola $n = p \cdot q$. La chiave segreta è $K_S^A = (p, q)$ mentre la chiave pubblica è $K_P^A = n$

2. B invia ad A il messaggio m usando la funzione di cifratura

$$f_A : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$f_A(m) = m^2 \bmod n$$

   quindi $c = m^2 \bmod n$ è il messaggio cifrato da B ed inviato ad A

3. A, per decifrare c, deve "estrarre la radice quadrata di $c \bmod n$", cioè deve determinare m tale che $m^2 \bmod n$. Allora:

   a) calcola:

$$m_p = c^{\frac{p+1}{4}} \bmod p \qquad \text{tale che} \qquad m_p^2 = c \bmod p$$
$$m_q = c^{\frac{q+1}{4}} \bmod q \qquad \text{tale che} \qquad m_q^2 = c \bmod q$$

   Infatti vale il teorema:

$$p \equiv 3 \bmod 4 \Rightarrow$$
$$\Rightarrow x^2 \equiv y \bmod p \Leftrightarrow x \equiv y^{\frac{p+1}{4}} \qquad y \neq g, \text{ con } < g >= \mathbb{Z}_p^*$$

   La proposizione consente di calcolare $x^2 \equiv y \bmod p$ a meno che la y non sia un generatore di $\mathbb{Z}_p^*$. Si veda a proposito l'es. 3.12

   b) osserva che anche $-m_p \bmod p$ è radice di c in $\mathbb{Z}_p$ e $-m_q \bmod q$ è radice di c in $\mathbb{Z}_q$. Quindi $\mp m_p \bmod p$ e $\mp m_q \bmod q$ sono le radici quadrate di c in $\mathbb{Z}_p$ e in $\mathbb{Z}_q$.

   c) poiché $(p, q) = 1$, per l'algoritmo di Euclide $\exists a, b \in \mathbb{Z}$ tale che $ap + bq = 1$

   d) Dato il teorema cinese del resto:

Esempio 3.12 Calcolare $x^2 \equiv 4 \bmod 7$

$\mathbb{Z}_7^*$ avrà $\varphi(6) = |\{1,5\}| = 2$ generatori. I generatori di $\mathbb{Z}_7^*$ saranno quindi $g = 3, 5$. Poiché 5 è un generatore allora la regola $x = 5^{\frac{p+1}{4}}$ non vale. Infatti si ottiene:

$$\begin{aligned} x &= 5^{\frac{p+1}{4}} \\ &= 5^{\frac{7+1}{4}} \\ &= 5^2 \\ &= 4 \end{aligned}$$

Ma $4^2 \neq 5 \bmod 7$.

Teorema 3.6. Teorema cinese del resto
Il sistema di congruenze lineari

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \end{cases} \qquad (n_1, n_2) = 1$$

ha un'unica soluzione

$$x_0 = (a_2 n_1 \lambda_1 + a_1 n_2 \lambda_2) \bmod n_1 n_2$$

con $\lambda_1, \lambda_2 \in \mathbb{Z}$ tali che valga l'algoritmo di Euclide tra n_1 e n_2:

$$n_1 \lambda_1 + n_2 \lambda_2 = 1$$

applica il teorema cinese del resto ai seguenti sistemi di congruenza lineari:

$$\begin{cases} x \equiv m_p \bmod p \\ x \equiv m_q \bmod q \end{cases} \qquad \begin{cases} x \equiv -m_p \bmod p \\ x \equiv m_q \bmod q \end{cases}$$

$$\begin{cases} x \equiv m_p \bmod p \\ x \equiv -m_q \bmod q \end{cases} \qquad \begin{cases} x \equiv -m_p \bmod p \\ x \equiv -m_q \bmod q \end{cases}$$

Le cui soluzioni sono rispettivamente:

$$\begin{aligned} m_1 &= m_q ap + m_p bq & \qquad m_2 &= m_q ap - m_p bq \\ m_3 &= -m_q ap + m_p bq & \qquad m_4 &= -m_q ap - m_p bq \end{aligned}$$

Uno di questi valori è il messaggio m inviato da B ad A e decifrato da A. Per determinare quello corretto si leggono i messaggi e solo uno avrà senso. In alternativa, si ovvia al problema del controllo manuale inserendo un testo preconcordato tra A e B in testa al messaggio.

3.5.1 Esempio di utilizzo

Di seguito viene riportato un esempio:

1. A sceglie $p = 3$ e $q = 7$. Infatti:

$$p \equiv 3 \bmod 4 \qquad 3 = 3 + 4 \cdot 0$$
$$q \equiv 3 \bmod 4 \qquad 7 = 3 + 4 \cdot 1$$

   Quindi si ha $n = 3 \cdot 7 = 21$, $K_S^A = (3, 7)$ e $K_P^A = 21$.

2. B vuole inviare $m = J$. In ASCII risulta $m = 10$. B cifra con la chiave pubblica di A:

$$c = m^2 \bmod n$$
$$c = 10^2 \bmod 21 = 16 \bmod 21$$

   Il messaggio inviato è quindi $c \equiv 16 \bmod 21$.

3. per decifrare, A deve determinare m tale che $m^2 \equiv 16 \bmod 21$

   a) A conosce la sua chiave segreta $K_S^A = (3, 7)$ e calcola m_3 e m_7. In $\mathbb{Z}_{21}$ (si noti che non è un campo, poiché 21 non è un numero primo) risulta $x^2 \equiv 16 \bmod 21 \quad x = m$. L'equazione ha 4 radici. Si può risolvere esaustivamente calcolando il quadrato di ogni elemento di $\mathbb{Z}_{21}$:

1^2	1	20^2
2^2	4	19^2
3^2	9	18^2
4^2	$\boxed{16}$	17^2
5^2	4	16^2
6^2	15	15^2
7^2	7	14^2
8^2	1	13^2
9^2	18	12^2
10^2	$\boxed{16}$	11^2

   Allora $x = [4, 10, 11, 17]$ sono le soluzioni di $x^2 \equiv 16 \bmod 21$.
   La ricerca esaustiva non sarebbe possibile con numeri molto grandi. Si sfrutta quindi la proposizione sulle radici quadrate:

$$p \equiv 3 \bmod 4 \Rightarrow$$
$$\Rightarrow x^2 \equiv y \bmod p \Leftrightarrow x \equiv y^{\frac{p+1}{4}} \qquad y \neq g, \text{ con } < g >= \mathbb{Z}_p^*$$

   In $\mathbb{Z}_3^*$ i generatori sono $\varphi(2) = 1$, ovvero $g = 2 \in \mathbb{Z}_3^*$. In $\mathbb{Z}_7^*$ i generatori sono $\varphi(6) = |\{1, 5\}| = 2$, ovvero $g = 3, 5 \in \mathbb{Z}_7^*$.

   $m_3 = c^{\frac{p+1}{4}} \bmod p = 16^{\frac{3+1}{4}} \bmod 3 = 1 m_7 = c^{\frac{q+1}{4}} \bmod q = 16^{\frac{7+1}{4}} \bmod 7 = 4$

b) le radici quadrate di c in $\mathbb{Z}_p$ e in $\mathbb{Z}_q$ sono $\mp m_p \bmod p$ e $\mp m_q \bmod q$. Quindi sono: $\mp m_3 \bmod 3 = 1 \bmod 3$ e $\mp m_7 \bmod 7 = 4 \bmod 7$

c) poiché $(3, 7) = 1$, per l'algoritmo di Euclide $\exists a, b \in \mathbb{Z}$ tale che $3a + 7b = 1$. Risulta $a = -2$ e $b = 1$, poiché $3(-2) + 7(1) = 1$

d) Applichiamo il teorema cinese del resto:

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 7 \end{cases} \qquad \begin{cases} x \equiv -1 \bmod 3 \\ x \equiv 4 \bmod 7 \end{cases}$$

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv -4 \bmod 7 \end{cases} \qquad \begin{cases} x \equiv -1 \bmod 3 \\ x \equiv -4 \bmod 7 \end{cases}$$

Le cui soluzioni sono rispettivamente:

$$\begin{aligned} m_1 &= m_q ap + m_p bq = 4 \cdot (-2) \cdot 3 + 1 \cdot 1 \cdot 7 = -17 =_2 1 = 4 \\ m_2 &= m_q ap - m_p bq = 11 \\ m_3 &= -m_q ap + m_p bq = 10 \\ m_4 &= -m_q ap - m_p bq = 17 \end{aligned}$$

3.6 Crittosistema di El-Gamal

Nel crittosistema di El-Gamal:

1. abbiamo due utenti A e B, un primo grande p ($\mathbb{Z}_p^*$) e un generatore g di $\mathbb{Z}_p^*$, ossia scelgono $< g >= \mathbb{Z}_p^*$
2. ciascun utente sceglie la chiave privata $x \in \mathbb{Z}_p^*$ e pubblica g^x
3. per inviare un messaggio m a B, A sceglie $k \in \mathbb{Z}_p^*$. Supponendo che l'uente B abbia chiave pubblica g^y, A calcola g^k e lo applica alla chiave pubblica del destinatario ottenendo $(g^y)^k = g^{yk}$ ed invia a B la coppia (g^k, mg^{yk})
4. per decifrare, B calcola $(g^{yk})^{-1}$:

$$(g^k)^y = g^{yk} \Rightarrow g^{-yk} = (g^{yk})^{-1}$$

Determina il messaggio m:

$$(m \cdot g^{yk})g^{-yk} = m(g^{yk-yk}) = m$$

3.7 Curva ellittica

Definizione 3.12. *Si dice* curva ellittica *l'insieme dei punti del piano $p(x, y)$ le cui coordinate soddisfano un'equazione cubica del tipo:*

$$y^2 = a_1x^3 + a_2x^2 + a_3x + a_4 \qquad a_1 \neq 0 \text{ e } a_1, a_2, a_3, a_4 \in \mathbb{R}$$

In particolare useremo curve ellittiche con equazione

$$y^2 = x^3 + ax + b \qquad a, b \in \mathbb{R}$$

e si indicheranno con $E(a, b)$.

Proposizione 3.4. $(E, +)$ *è un* gruppo Abeliano *nel quale* O *è l'identità:*

$$\forall P \in E \qquad P + O = O + P = P$$

Dimostrazione. Data una curva E vogliamo calcolare $P + Q$ con $P = (x_1, y_1)$ e $Q = (x_2, y_2)$. Consideriamo tre casi:

1. $x_1 \neq x_2$.

   La retta passante per P e per Q interseca E in un terzo punto R'. Sia R il simmetrico di R', risulta $P + Q = R$

2. $x_1 = x_2$ e $y_1 = -y_2$

   In questo caso $P + Q = O$. Poiché risulta quindi:

   $$(x, y) + (x, -y) = O$$

   allora $(x, -y)$ è *l'inverso* di (x, y) rispetto alla somma di due punti

3. $x_1 = x_2$ e $y_1 = y_2$

   Nel terzo caso, stiamo sommando P a se stesso. Il terzo caso viene trattato come il primo, con la differenza che stavolta la retta è la tangente ad E nel punto P.

□

In crittografia non si usano curve su $\mathbb{R}$, ma quelle su GF(p) e GF(2^n). Non sembra esserci differenza tra la sicurezza offerta dai campi GF(p) e GF(2^n). Le realizzazioni su GF(p) sono le migliori per le applicazioni software poiché non richiedono numerosi operazioni, mentre le realizzazioni su GF(2^n) sono le migliori per le applicazioni hardware poiché bastano pochi elementi per creare un sistema veloce e potente. Le curve su GF(p) sono definite esattamente come quelle su $\mathbb{R}$; le operazioni su $\mathbb{R}$ vengono sostituite con le analoghe operazioni su GF(p). La curva è formata da tutti i punti (x, y) che soddisfano la congruenza:

$$y^2 \equiv (x^3 + ax + b) \bmod p \qquad p \text{ primo e } a, b \in \mathbb{Z}_p$$

L'insieme dei punti del piano che soddisfano questa equazione si chiama *curva ellittica su* $\mathbb{Z}_p$ e si indica con $E_p(a, b)$.

Proposizione 3.5. $(E_p, +)$ *è un* gruppo Abeliano

Dimostrazione. Rispetto alla proposizione 3.4 ci sono due differenze:

- la somma $x + y$ corrisponde al prodotto mod$n$ in RSA (xor bit a bit)

Esempio 3.13 Scrivere la curva ellittica $E_{23}(1,1)$

Risulta $p = 23$ e $a = b = 1$. Quindi:

$$y^2 = (x^3 + x + 1) \bmod 23$$

- l'inverso di un punto (x, y) è il punto $(x, x + y)$

□

Teorema 3.7. Teorema di Hasse
Sia $E_p(a,b)$ una curva ellittica su $\mathbb{Z}_p$. Allora la cardinalità $\operatorname{card} E_p(a,b)$ *è tale che*

$$p + 1 - 2\sqrt{p} \leq \operatorname{card} E_p(a,b) \leq p + 1 + 2\sqrt{p}$$

Per p molto grande risulta:

$$\operatorname{card} E_p(a,b) \cong \mathbb{Z}_p$$

Quindi non c'è molta sicurezza poiché il problema del logaritmo discreto è risolubile. Bisogna scegliere opportune curve ellittiche.

3.7.1 Crittosistemi basati su curve ellittiche

I crittosistemi basati su curve ellittiche sembrano offrire lo stesso livello di sicurezza dei crittosistemi a chiave pubblica tradizionali. Le chiavi infatti sono molto più corte e comporta una maggiore velocità per cifratura/decifratura, una memorizzazione efficiente e un minore utilizzo della larghezza di banda.

Il concetto di fondo è il seguente:

Proposizione 3.6. *Dato un punto B su una $E_p(a,b)$ risulta semplice calcolare* $\underbrace{p + \ldots + p}_{k \text{ volte}}$ *(funzione di cifratura f). Ma, dato un punto $P \in E_p(a,b)$, è difficile trovare un intero k tale che $kB = P$*

Definizione 3.13. *Dato un punto $P \in E_p(a,b)$, l'intero k tale che $kB = P$ è detto il* logaritmo (discreto) *di P in base B*

Proposizione 3.7. *Il multiplo di un punto corrisponde al logaritmo discreto*

3.8 Crittografia quantistica

Definizione 3.14. *I* quanti *sono le più piccole particelle fisiche*

Ad esempio i fotoni sono quanti di energia elettromagnetica. Muovendosi nello spazio vibrano secondo un angolo di vibrazione detto *polarizzazione*. Per semplicità consideriamo solo gli angoli 0°, 45°, 90°, 135°. Un *calcolatore quantistico* si basa su bit

quantistici, i *qubit*. Usando i qubit si potrebbero eseguire moltissimi calcoli in pochi istanti. Per esempio, con 250 qubit si avrebbero 10^75 stati ($2^250 \cong 10^75$).

Nel calcolatore si avrebbe una sovrapposizione di stati. I problemi per la costruzione di un calcolatore quantistico sarebbero:

- conservare lo stato di sovrapposizione quantistica per tutto il tempo in cui lavora, perché la sovrapposizione esiste solo in assenza di osservazione o di qualunque altra interazione.
- riuscire a programmarlo per la lettura delle sovrapposizioni: risulta impossibile distinguere i casi in cui l'errore introdotto sia dovuto ad un "origliamento" della spia oppure ad un errore sperimentale sempre presenti in una misura reale.

Teorema 3.8. Principio di indeterminazione di Heisenberg

Non è possibile conoscere simultaneamente e con precisione assoluta coppie particolari di proprietà di un oggetto, per esempio la posizione e la velocità di un elettrone oppure uno stato di polarizzazione o un altro stato non perpendicolare di un fotone

L'esperimento di *Yang* si può effettuare con una sorgente capace di emettere un fotone alla volta che può attraversare solo una delle due feniliture. Dopo un'ora, sullo schermo ci aspettiamo solo luce, invece si ottiene ancora lo schermo a strisce poiché vale il principio di sovrapposizione.

3.8.1 Ipotesi della sovrapposizione

Poiché non si conosce la traiettoria del fotone tra la sorgente e lo schermo, il fotone può essere passato da entrambe le fenditure, interagendo con sé stesso (emphautointerferenza) dà origine allo schermo a strisce.

L'algoritmo quantistico *BB84* (Bennet–Brassard 1984)

$$\text{Schema diagonale } \times \begin{cases} \text{fotone polarizzato } \diagup & \text{indice 1} \\ \text{fotone polarizzato } \diagdown & \text{indice 0} \end{cases}$$

$$\text{Schema rettilineo } + \begin{cases} \text{fotone polarizzato } \updownarrow & \text{rappresenta 1} \\ \text{fotone polarizzato } \leftrightarrow & \text{rappresenta 0} \end{cases}$$

Riportando l'algoritmo quantistico nel contesto crittografico, risulta:

1. A rappresenta i bit con fotoni polarizzati (schema + o $\times$). A invia a B una sequenza di fotoni che B misura con schema + o con schema $\times$. Se B dovesse scegliere la misura sbagliata rispetto alla base usata da A, il risultato della misura sarà casuale, ovvero 0 oppure 1 con probabilità del 50%. Il punto cruciale è che anche un eventuale attaccante si troverebbe nella stessa situazione di B: infatti quando la spia intercetta i fotoni dovrà anch'essa scegliere tra le due misure possibili e se sceglie quella sbagliata ottiene un risultato casuale.
2. A e B controllano quali misure fatte da B sono corrette. A comunica a B solo il tipo di schema di polarizzazione, non il risultato che B avrebbe dovuto ottenere.

3. A e B scartano le misure di B non corrette e usano quelle corrette. Creano così una chiave comune a blocco monouso. Se un attaccante interferisce, egli, osservando i fotoni, per il principio di indeterminazione, ne modifica lo stato.

4. A e B controllano l'integrità della loro chiave comune confrontando i bit non scartati se il risultato è uguale per entrambi, usano questa chiave per cifrare. Per essere sicuri che la spia non ha intercettato la chiave basta notare che se questa avesse in qualche modo intercettato i fotoni nel loro tragitto tra A e B, per il principio d'indeterminazione, ne avrà necessariamente modificato le caratteristiche introducendo quindi degli errori nella misura di B anche nei bit che dovrebbero risultare corretti. Quindi, se dopo aver scartato i bit, la chiave di B risulta diversa da quella di A, vuol dire che la spia ha intercettato i fotoni e che la chiave non è sicura.