CRITTOGRAFIA

La parola crittografia deriva dall'unione di due parole greche: kryptos= nascosto e graphia=scrittura.

La crittografia si occupa di scritture nascoste. L'idea fondamentale è di non rendere accessibili i dati a chi non è autorizzato e quindi bisogna modificare la scrittura, ovvero cifrarla, nasconderla.

Il problema che vogliamo affrontare è il seguente. Ci sono due utenti: A=Alice e B=Bob e Alice vuole comunicare in maniera segreta con Bob

$$A \quad \stackrel{M}{\rightarrow} \quad B.$$

Quindi, Alice vuole spedire un messaggio M in modo che non sia comprensibile, letto da nessun'altro se non Bob. Pertanto, Alice non può spedire M cosi come è, ma deve necessariamente modificarlo, ovvero cifrarlo, in modo che non venga capito da nessuno diverso da Bob.

Per prima cosa questo è un nostro diritto!! Articolo 15 della Costituzione Italiana:

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Inoltre, rendere il messaggio nascosto è ormai necessario. Ad esempio, serve per:
-spedire mail;
-fare acquisti tramite carta di credito;
-avere un indirizzo di posta elettronica;
-criptare segnali radio o pay tv (nessuno pagherebbe più abbonamenti).
Inoltre, è stato sempre necessario per scopi militare.

Quindi l'idea fondamentale è:
A non spedisce un messaggio in chiaro ma lo deve prima criptare e modificare e dopo spedisce il messaggio cifrato;
B riceve il messaggio cifrato e deve decifrarlo e vogliamo che solo B riesca a capire il messaggio!

0.1. **Parole e numeri.** Ad ogni lettera possiamo associare un numero. Per far questo ci sono vari modi:
- possiamo numerarle partendo da $A = 1,\ B = 2...$;
- possiamo far corrispondere alla lettera A il numero 065 e alla lettera Z il numero 090. Questo è il codice *ASCII= American Standard Code for Information Interchange.*

Quindi possiamo pensare di dover comunicare in maniera segreta e sicura un numero.

Ci sono varie tecniche usate in crittografia. La prima grande distinzione dei sistemi crittografici è di due tipi: *sistemi a chiave privata e sistemi a chiave pubblica.*

La crittografia a chiave privata, prevede l'utilizzo di una chiave privata che deve essere comunicata per decifrare il testo. Quindi il problema è dover comunicare, in maniera segreta e sicura, questa chiave privata.

I crittografi, matematici e ingegneri si sono chiesti: è possibile solo con una chiave privata la cifratura? Non si può evitare di dover spedire la chaive privata?

La risposta è si, e questi sistemi in cui non si deve spedire alcuna chiave privata sono detti crittografia a chiave pubblica.

L'introduzione dei sistemi a chiave pubblica è avvenuta negli anni '70 ed è stata una vera rivoluzione all'interno della crittografia.

0.2. **Sistema RSA.** Nel 1975 Diffie (crittografo e avvocato) e Hellmann (ingegnere elettrico) introducono l'idea di usare una chiave pubblica.

L'idea è stata poi sviluppata e pubblicata nel 1976 da tre ricercatori del MIT: Rivest Shamir e Adleman, da cui prende il nome: sistema RSA. Il sistema RSA è un sistema per crittografare. È un sistema a chiave pubblica, ovvero non necessita lo scambio di chiavi private per cifrare e decifrare un messaggio (altrimenti avremmo comunque il problema di spedire la chiave privata). La conoscenza della chiave pubblica e dell'algoritmo di cifratura, anch'esso pubblico, non basta per risalire alla chiave privata in tempi brevi.

Viene detto sistema a crittografia asimmetrica: ci sono due chiavi distinte una per cifrare e una per decifrare che sono legate tra loro, ma conoscendone una non si riesce a trovare l'altra.

Tutta la segretezza si base sul difficile *problema di fattorizzare un numero come prodotto di potenze di primi distinti.*

Vediamo come funziona.

Abbiamo i due utenti Alice e Bob.

Alice sceglie due numeri (n_A, e_A) e lo stesso fa Bob (n_B, e_B).

Questi numeri sono pubblici, disponibili a tutti. Ci sono elenchi pubblici certificati con queste chiavi pubbliche.

Le prorietà dei numeri sono:

n è prodotto di due numeri primi molto grandi (migliaia di cifre). Quindi

$$n_A = p_A q_A \qquad n_B = p_B q_B.$$

I numeri n_A e n_B sono pubblici mentre la loro fattorizzazione in primi no.

Dopo aver scelto n_A, Alice sceglie e_A in modo che non abbia fattori in comune con $\varphi(n_A) = (p_A - 1)(q_A - 1)$, dove φ è la funzione di Eulero.

I numeri (n_A, e_A) e (n_B, e_B), sono noti a tutti, i numeri e_A e e_B sono anche detti chiavi pubbliche.

Alice è in possesso di una chiave privata (!) che non deve comunicare e non serve comunicare per far decifrare il suo messaggio.

La chiave privata di Alice è il valore d_A che risolve la congruenza lineare

$$e_A x \equiv 1 \pmod{\varphi(n_A)}.$$

La congruenza lineare si riesce a risolvere (in tempi ragionevoli) solo da Alice che ha a disposizione p_A e q_A. Infatti, $\varphi(n_A) = \varphi(p_A q_A) = (p_A - 1)(q_A - 1)$ e quindi la congruenza per Alice è

$$e_A x \equiv 1 \pmod{\varphi(n_A) = (p_A - 1)(q_A - 1))}.$$

Inoltre, poiché Alice ha scelto e_A in modo che non ha fattori in comune con $\varphi(n_A) = (p_A - 1)(q_A - 1)$, si ha che la soluzione della congruenza è unica: la chiave priva d_A. Il numero d_A è detto anche inverso di e_A modulo $(p_A - 1)(q_A - 1)$.

Dire che $e_A d_A \equiv 1 \pmod{\varphi(n_A)}$, implica che esiste un numero s tale che

$$e_A d_A = s \cdot \varphi(n_A) + 1. \tag{1}$$

Bob fa la stessa cosa. Anche lui ha una chiave privata d_B che risolve la congruenza lineare

$$e_B x \equiv 1 \pmod{\varphi(n_B)} \text{ ovvero } e_B \cdot d_B \equiv 1 \pmod{\varphi(n_B)}.$$

Ricordiamo che questo significa che il resto del numero $e_B \cdot d_B$ nella divisione per $\varphi(n_B)$ è 1, ovvero che esiste un numero t tale che

$$e_B \cdot d_B = t\varphi(n_B) + 1. \tag{2}$$

A questo punto Alice ha il suo messaggio M, lo trasforma in numero e sull'elenco controlla i numeri di Bob (n_B, e_B).

Spezza M in vari messaggi, con numero di cifre minori delle cifre di n_B.

Successivamente, calcola la potenza M^{e_B} e ne calcola il resto C nella divisione per n_B, ovvero

$$M^{e_B} \equiv C \pmod{n_B}.$$

Ricordiamo che i numeri n_B ed e_B sono pubblici e quindi Alice riesce a trovare il numero C, è il resto di una divisione: è il resto di M^{e_B} nella divisione per n_B.

A questo punto, Bob non riceve il messaggio in chiaro M, ma riceve il testo cifrato C. Cosa fa?

Prende la sua chiave privata d_B e considera la potenza C^{d_B} e determina la classe resto di questo numero C^{d_B} modulo n_B, ovvero

$$C^{d_B} \equiv? \pmod{n_B}.$$

Questo Bob lo sa calcolare, perché non è altro che il resto della divisione di C^{d_B} diviso n_B. Ma a cosa corrisponde questo resto?

Ricordiamoci che $M^{e_B} \equiv C \pmod{n_B}$ e quindi $M^{e_B \cdot d_B} \equiv C^{d_B} \pmod{n_B}$ ed inoltre l'Equazione 2 ci dice che $e_B \cdot d_B = t\varphi(n_B) + 1$, per qualche t. Ne segue che

$$C^{d_b} \equiv M^{e_b d_b} \equiv M^{t\varphi(n_B)+1} \equiv M^{t\varphi(n_B)} \cdot M^1 \equiv M^{t\varphi(n_B)} \cdot M \equiv 1 \cdot M \equiv M \pmod{n_B}.$$

Nell'ultima congruenza come abbiamo fatto a sostituire $M^{t\varphi(n_B)}$ con 1? Ovvero come possiamo dire che $M^{t\varphi(n_B)} \equiv 1 \pmod{n_B}$? Questo è dovuto al Teorema di Eulero-Fermat ($a^{\varphi(n)} \equiv 1 \pmod{n}$ e quindi ($a^{t\varphi(n)} \equiv 1^t \equiv 1 \pmod{n}$).

La chiave per cifrare è una chiave pubblica e_B, nota a tutti; mentre quella per decifrare è una chiave privata d_B e NON serve trasmetterla.

0.3. **Firma.** Nel caso di chiave pubblica, c'è un problema: poiché la chiave è pubblica, tutti possono spedire a Bob un messaggio cifrato e far finta di essere Alice.

Quindi bisogna aggiungere una sicurezza: una firma che è legata all'utente A, che serve per capire se effettivamente Alice ha mandato il messaggio.

Ovviamente la firma deve dipendere da qualcosa che ha solo Alice e solo lei può fare: ovviamente dipende dalla sua chiave privata d_A!

Ad esempio Alice scrive il suo nome o un suo codice e lo traduce in un numero F cheè la sua firma.

Allora procede nel seguente modo. Considera il resto di F^{d_a} nella divisione con n_A, ovvero risolve la congruenza

$$F^{d_a} \equiv T \pmod{n_A}.$$

Il numero d_a non è pubblico e quindi solo Alice può calcolare la potenza e il resto T.

A questo punto Alice spedisce il messaggio cifrato T.

Bob riceve T e cosa fa? Usa la chiave pubblica di Alice, ovvero il numero e_A per considerare la potenza T^{e_A}. Poi ne calcola il resto nella divisione per n_A. Ricordiamoci che $T^{e_a} \equiv F^{d_A e_A} \pmod{n_A}$. Quindi

$$T^{e_a} \equiv F^{d_A e_A} \equiv F^{s\cdot\varphi(n_A)+1} \equiv F^{s\cdot\varphi(n_A)} \cdot F^1 \equiv F^{ts\cdot\varphi(n_A)} \cdot F \equiv 1 \cdot F \equiv F \pmod{n_A},$$

usando l'Equazione 1 e applicando di nuovo il Teorema di Eulero-Fermat.

In questo modo, Bob controlla che il messaggio decifrato corrisponde ad F e capisce che effetivamente è stata Alice a spedirlo.