Cos'è la critografia?

È la scienza che si occupa di proteggere i dati trasformandoli matematicamente in un formato non leggibile.

A cosa serve?

- A proteggere delle informazioni riservate che devono restare tali;
- Per garantire l'autenticità di un documento;
- Aiuta a preservare la nostra privacy;
- Offre degli stumenti per l'e-commerce
- ...

La crittografia non è una scoperta recente

- Nel 400 a.C a Sparta veniva usato un bastone avente un certo diametro, chiamato *scitala*.

  Esempio (con scitala di altezza pari a 5 caratteri e circonferenza pari a 9).
  Testo in chiaro: ALLE PROSSIME ELEZIONI MI PRESENTO ANCHE IO
  Cifratura:

  $$\begin{array}{ccccccccc} A & P & I & L & N & & E & A & I \\ L & R & M & E & I & P & N & C & O \\ L & O & E & Z & & R & T & H & \\ E & S & & I & M & E & O & E & \\ & S & E & O & I & S & & & \end{array}$$

  Testo cifrato: APILN EAILRMEIPNCOLOEZ RTH ES IMEOE SEOIS

- Ancora nell'antica Grecia, veniva usato il disco di Enea il Tattico, un particolare disco con 24 fori, uno per ogni lettera dell'alfabeto. La codifica del messaggio avveniva passando un filo attraverso i fori corrispondenti alle differenti lettere. Srotolando il filo, avveniva la lettura al contrario del messaggio.

- Giulio Cesare per comunicare con i propri eserciti usava il seguente metodo che consisteva nello scrivere i messaggi spostando tutte le lettere dell'alfabeto di 3 posizioni: A con D, B con E, ... , Z con C. Tale sistema è noto come cifrario monoalfabetico.
  Esempio (con alfabeto a 21 caratteri).

Messaggio in chiaro:	`DE BELLO GALLICO`
Messaggio cifrato:	`GH EHOOR LDOONFR`

- Augusto introdusse un sistema di cifratura più complesso di quello di Cesare, che utilizzava per scrivere un messaggio il testo scritto in un libro, per esempio l'Odissea.

- La prima macchina di cui si ha notizia (fine '800) è il disco di Wheatstone, un sistema formato da due dischi concentrici

- Durante la seconda guerra mondiale i tedeschi utilizzavano una macchina di cifratura chiamata Enigma, composta di vari dischi che ruotavano alla pressione di ogni tasto. Nonostante i tedeschi la considerassero inattaccabile, gli inglesi costruirono una macchina chiamata Colossus in grado di decifrarne i messaggi.

Crittografia a chiave simmetrica: una chiave

- La chiave di cifratura coincide con quella di decifratura;

- Le chiavi risultano note ad entrambi i partner;

- Entrambi i partner devono tenere segreta la chiave, l'integrità del sistema dipende da entrambi;

- Ci possono essere delle difficoltà per quanto riguarda lo scambio delle chiavi;

- La chiave si calcola in tempi rapidi;

Crittografia a chiave pubblica: due chiavi

- La chiave di cifratura è diversa dalla chiave di decifrazione;

- La chiave di cifratura può essere nota a tutti, per cui può essere resa pubblica dal destinatario;

- La chiave di decifrazione è mantenuta segreta dal destinatario ed è nota soltanto a lui;

- Fornisce un metodo per realizzare la firma digitale;

- La tecnica si basa sul lavoro teorico che elaborarono nel 1976 due crittologi americani, Diffie ed Hellmann;

- La crittografia RSA è il primo esempio pratico di tale lavoro. (Rivest, Shamir e Adleman).

Utilizzo della crittografia a chiave pubblica per le firme digitali

Con una firma digitale gli autori di un messaggio, di un file o di altri dati codificati in modo digitale possono associare la propria identità alle informazioni, ovvero apporvi una firma. In genere, le firme digitali si utilizzano quando i dati vengono diffusi come testo in chiaro, è comunque importante assicurare che il formato dei dati sia quello originale e che le informazioni non siano state inviate da un impostore.

Per garantire autenticità ed integrità, le trasmissioni di un sistema a chiave pubblica devono soddisfare $P_A(S_A(M)) = M$. Supponiamo che A voglia mandare un messaggio autentico a B. Allora:

- A calcola la sua firma digitale $C = S_A(M)$;
- Spedisce la coppia (M, C) (messaggio, firma);
- Quando B riceverà la coppia (M, C) può verificare che questo provenga da A essendo P_A

la chiave pubblica di A, verificando l'equazione $M = P_A(C)$.

Così B può accertare che il messaggio è stato spedito da A e non è stato alterato.

Algoritmi hash unidirezionali

Un hash è la conversione di un segmento di dati di qualsiasi lunghezza in un numero a lunghezza fissa non reversibile, tramite l'applicazione ai dati di una funzione matematica unidirezionale, chiamata algoritmo hash.

Firma digitale: combinazione di chiave pubblica e hash

È possibile utilizzare la tecnologia a chiave pubblica unitamente agli algoritmi hash, per creare una firma digitale che consenta di verificare l'integrità dei dati e di dimostrare il possesso della chiave privata.

Le operazioni necessarie per la firma e la verifica dei dati eseguite da applicazioni che supportano l'infrastruttura a chiave pubblica sono le seguenti:

- Il mittente applica un algoritmo hash ai dati, generando un valore hash.

- Utilizzando una chiave privata, il mittente trasforma il valore hash in una firma digitale.

- Il mittente invia i dati, la firma e il proprio certificato al destinatario.

- Il destinatario applica l'algoritmo hash ai dati ricevuti e genera un valore hash.

- Il destinatario utilizza la chiave pubblica del firmatario e il valore hash appena generato, per verificare la firma.

Scambio di chiave: combinazione di chiave simmetrica e chiave pubblica

Gli algoritmi a chiave simmetrica sono eccellenti per crittografare i dati in modo rapido e sicuro. Tuttavia, il loro punto debole è costituito dal fatto che il mittente e il destinatario devono scambiarsi una chiave segreta prima che sia possibile scambiare i dati. Le operazioni necessarie per uno scambio di chiave basato su chiave pubblica sono le seguenti:

- Il mittente ottiene la chiave pubblica del destinatario.

- Il mittente crea una chiave segreta casuale (la singola chiave utilizzata nella crittografia a chiave simmetrica).

- Il mittente utilizza la chiave segreta con un algoritmo simmetrico, per convertire il testo normale in testo crittografato.

- Il mittente utilizza la chiave pubblica del destinatario per trasformare la chiave segreta in una chiave segreta crittografata.

- Il mittente invia il testo e la chiave segreta crittografati al destinatario.

- Il destinatario converte la chiave segreta crittografata in testo normale utilizzando la propria chiave privata.

- Il destinatario converte il testo crittografato in testo normale utilizzando la chiave segreta non crittografata.

Il metodo crittografico RSA divide i messggi in blocchi. Ogni blocco viene considerato come un numero intero. Ogni blocco viene passato ad una particolare funzione che deve essere del tipo a trabocchetto. Una funzione è detta a trabocchetto quando è facile da calcolare ma difficile da invertire, sempre che non si possieda un'informazione segreta aggiuntiva.
Un esempio di funzione ritenuta a trabochetto è: $f(x) = x^a \ mod \ n$ dove n è il prodotto di due primi p e q abbastanza grandi, a è un intero positivo ed $f : \mathbb{Z}_n \to \mathbb{Z}_n$

Per consentire la trasmissione di un messaggio da A a B, in sicurezza, le trasformazioni di un sistema a chiave pubblica devono soddisfare $M = S_B(P_B(M))$. Supponendo che A voglia spedire un messaggio M in maniera sicura a B. Allora:

- A ottiene la chiave pubblica di B, P_B;

- A calcola il testo cifrato $C = P_B(M)$ corrispondente al messaggio M e lo spedisce a B;

- B riceve il testo cifrato C e adopera la sua chiave privata S_B per ottenere il messaggio M, $S_B(C) = S_B(P_B(M)) = M$.

Generazione delle chiavi

1. A genera due numeri primi grandi p e q;

2. A calcola $n = p \cdot q$ e $\Phi(n) = (p-1)(q-1)$;

3. A sceglie un numero $1 < e < \Phi(n)$ tale che $gcd(e, \Phi(n)) = 1$;

4. A calcola $d = e^{-1} \ mod \ \Phi(n)$

5. A pubblica n ed e come sua chiave pubblica $P_A = (e, n)$;

6. A conserva n e d come sua chiave privata $S_A = (d, n)$.

Cifratura e decifratura

Per effettuare la cifratura di un messaggio $M \in \mathbb{Z}_n$, il mittente A preleva dall'elenco la chiave pubblica P_B dell'utente destinatario B e calcola il testo cifrato

$$C = P_B(M) = M^e \; mod \; n$$

Il destinatario conoscendo la sua chiave segreta $S_B = (d, n)$ calcola il messaggio in chiaro

$$M = S_B(C) = C^d \; mod \; n$$

Correttezza

Verifichiamo ora che la fase di cifratura e quella di decifratura sono una l'inversa dell'altra. Poiché

$$ed \equiv 1 \; mod \; \Phi(n)$$

si ha

$$ed = t \cdot \Phi(n) + 1$$

con t intero e $t \geq 1$. Supposto che $M \in \mathbb{Z}_n^*$, si ha:

$$C^d \; mod \; n = (M^e \; mod \; n)^d \; mod \; n =$$

$$= M^{t \cdot \Phi(n)+1} \; mod \; n = M$$

in quanto per il teorema di Eulero si ha che: $x^{\Phi(n)} = 1 \ mod \ n$. Nel caso in cui la lunghezza di M sia maggiore di n, si avrebbe che M e $(M \, mod \, n)$ originerebbero lo stesso crittogramma. Per ovviare a questo problema si assume che i messaggi siano numeri minori di n. Questo lo si può semplicemente ottenere decomponendo la sequenza di bit rappresentanti il messaggio in chiaro, in gruppi di $l = log_2 \ n$ bit ciascuno. Così facendo si garantisce che $m < 2^l < n$.

Esempio RSA con piccoli numeri

Generazione delle chiavi

- A sceglie due numeri primi p e q: $p = 47$, $q = 71$;

- A calcola $n = p \cdot q$ e $\Phi(n) = (p-1) \cdot (q-1)$
  $n = 47 \cdot 71 = 3337$, $\Phi(n) = 46 \cdot 70 = 3220$
  A sceglie e tale che $gcd(e, \Phi(n)) = 1$ $e = 79$
  A calcola $d = e^{-1} \ mod \ \Phi(n)$
  $d = 79^{-1} \ mod \ 3220 = 1019$

La chiave pubblica è la coppia $(e, n) = (79, 3337)$
La chiave privata è la coppia $(d, n) = (1019, 3337)$

Cifratura

- Un utente B spedisce ad A il messaggio $M = 688$ conoscendo la sua chiave pubblica $P_A = (79, 3337)$

- B calcola $C = M^e \ mod \ n$
$C = 688^{79} \ mod \ 3337 = 1570$

Decifratura

- A riceve il messaggio cifrato $C = 1570$

- A si ricava M con la formula $M = C^d \ mod \ n$
$M = 1570^{1019} \ mod \ 3337 = 688$

Computazioni di RSA

Le procedure del crittosistema RSA si basano sull'elevazione a potenza modulare e sulla risoluzione di equazioni modulari. Quindi bisogna usare deglia algoritmi efficienti per tali operazioni. Inoltre bisogna individuare numeri primi grandi in modo efficiente.

Sicurezza di RSA

- La sicurezza della RSA si basa sul fatto che la funzione di cifratura $x^e \ mod \ n$ è una funzione trabocchetto che è computazionalmente difficile da invertire;

- Solo conoscendo la fattorizzazione di n è possibile trovare il valore delle chiavi;

- Conoscendo la fattorizzazione di n è possibile calcolare $\Phi(n) = (p-1)(q-1)$ e calcolare $d = e^{-1} \ mod \ \Phi(n)$ usando l'algoritmo esteso di Euclide;

- Da ciò si deduce che la sicurezza della RSA dipende dal problema di fattorizzare grandi numeri;

- Il modo più ovvio di attaccare il sistema, è quello di tentare di risolvere quest'ultimo problema. Gli algoritmi più efficienti, conosciuti fino ad ora, hanno una complessità

$$O(e^{\sqrt{(\ln x)(\ln \ln x)}})$$

- Fattorizzare un numero di 664 bit richiede almeno 10^{23} passi usando gli algoritmi più efficienti; per cui ipotizzando di avere una rete costituita da un milione di computer che a testa eseguono un milione di passi al secondo, il tempo impiegato per fattorizzare n sarebbe dell'ordine dei 4000 anni. Se poi n fosse un numero a 1024 bit la stessa rete impiegherebbe 10^{10} anni per fattorizzarlo.

- Non è impossibile decifrare un testo cifrato con il crittosistema RSA, ma piuttosto è computazionalmente difficile.

Attacchi RSA

- Per un crittoanalista rompere la RSA equivale a calcolare $\Phi(n)$. Infatti, se n e $\Phi(n)$ sono conosciuti ed n è il prodotto di due primi p e q, n può essere facilmente fattorizzato risolvendo le due seguenti equazioni: $n = p \cdot q$ e $\Phi(n) = (p-1)(q-1)$;

- Sostituendo $q = n/p$ nella seconda equazione se ne ottiene un'unica di secondo grado nella sola incognita p:

$$p^2 - (n - \Phi(n) + 1)p + n = 0$$

- Le due radici di questa equazione sono i fattori p e q.