Crittografia Asimmetrica

Schema e Concetti Fondamentali La crittografia asimmetrica, o a chiave pubblica, si basa sull'uso di una coppia di

Chiave Pubblica (k_1 o K_{pub}): Può essere distribuita liberamente, anche su canali insicuri. Viene usata per cifrare i m

Chiave Privata (k_2 o K_{priv}): Deve essere mantenuta segreta dal suo proprietario. Viene usata per decifrare i messagg

Lo schema generico per la **confidenzialità** è il seguente:

Bob vuole inviare un messaggio m ad Alice.

Bob ottiene la chiave pubblica di Alice, K_{pubA} (es. tramite un canale insicuro).

Bob cifra il messaggio usando la chiave pubblica di Alice: $c = E_{K_{pubA}}(m)$.

Alice riceve il messaggio cifrato c.

Alice usa la sua chiave privata, K_{privA}, per decifrare il messaggio: $m = D_{K_{privA}}(c)$.

[H] [width=0.8]asymm-gen.png Schema generico crittografia asimmetrica

La proprietà fondamentale è che, data la chiave pubblica k_1, deve essere computazionalmente impossibile (molto di

Obiettivi e Basi Teoriche I meccanismi asimmetrici servono a tre scopi principali:

Confidenzialità: Proteggere il contenuto del messaggio (come visto sopra).

Firme Digitali: Fornire autenticazione del mittente, integrità del messaggio e non ripudio.

Instaurazione di Chiavi Effimere: Scambiare in modo sicuro una chiave di sessione (es. simmetrica), come fa il prot

Questi meccanismi basano la loro sicurezza sulla difficoltà (ad oggi) nel risolvere alcuni problemi della teoria dei nu

Semplici da calcolare: Es. $n = p \cdot q$ (moltiplicazione di due primi).

;Difficili da invertire: Es. trovare p e q dato n (fattorizzazione di interi).

La sicurezza non è provata in assoluto, ma si basa sul fatto che i problemi matematici sottostanti sono studiati da secoli

Richiami: Teorema di Eulero e Fondamenti di RSA

RSA si basa su proprietà dell'aritmetica modulare. Dato un intero positivo n, definiamo:

$Z_n = \{0, 1, 2, \ldots, n-1\}$, l'insieme dei resti mod n;

$Z_n^* = \{x \in Z_n \mid \gcd(x, n) = 1\}$, cioè i numeri "primi relativi" con n;

la **funzione di Eulero** $\phi(n) = |Z_n^*|$, cioè la quantità di numeri minori di n e coprimi con esso.

Alcuni casi notevoli:

Teorema di Eulero Per ogni $m \in Z_n^*$ vale:

Da cui segue il corollario fondamentale di RSA:

Se scegliamo due numeri e e d tali che

allora l'elevamento a potenza con e e con d sono operazioni inverse modulo n:

Questa è la base matematica che rende possibile RSA.

Algoritmo RSA (Rivest, Shamir, Adleman) RSA (1977) è il primo e più noto meccanismo asimmetrico "tuttofare",

Generazione delle Chiavi I parametri di RSA sono:

Parametri Privati (segreti):

Si scelgono due numeri primi p e q molto grandi (es. 512+ bit).

Si calcola $\phi(n) = (p-1)(q-1)$.

Si sceglie e (esponente pubblico) e si calcola d (esponente privato) tale che $d = e^{-1}\phi(n)$ (cioè $e \cdot d = 1\phi(n)$).

Parametri Pubblici (condivisibili):

Si calcola il modulo $n = p \cdot q$.

Si pubblica e (spesso un numero piccolo e fisso, come $e = 65537$).

La chiave pubblica è $K_{pub} = \{e, n\}$ e la chiave privata è $K_{priv} = \{d, n\}$.

Utilizzi di RSA

1. Confidenzialità Come nello schema generale: Bob cifra m per Alice usando la K_{pub} di Alice.

Cifratura (Bob): $c = m^e n$

Decifratura (Alice): $m = c^d n$

L'operazione funziona per il teorema di Eulero, purché $m < n$.

[H] [width=0.8]RSAconf.png Schema RSA per Confidenzialità

2. Firme Digitali Nelle firme RSA il mittente dimostra la proprietà della chiave privata:

Alice calcola il digest del messaggio: $h = H(m)$.

Alice firma il digest: $f = h^d n$.

Alice invia a Bob la coppia $\{m, f\}$.

Bob verifica la firma calcolando $h' = f^e n$ e confrontando h' con $H(m)$.

Se coincidono, Bob sa che:

il messaggio non è stato modificato (integrità);

il mittente è realmente Alice (autenticità);

Alice non può negare di averlo inviato (non ripudio).

[H] [width=0.8]RSAfirme.png Schema RSA per Firme Digiali 3. Instaurazione di Chiavi Effimere Poiché RSA è co

Bob genera una chiave simmetrica r (es. per DES o AES), detta chiave effimera o di sessione.

Bob cifra r usando la K_{pub} di Alice (RSA): $c = r^e n$.

Bob invia c ad Alice.

Alice decifra c con la sua K_{priv} (RSA) e ottiene r: $r = c^d n$.

Ora Bob e Alice condividono la chiave simmetrica r e la usano per cifrare il resto della comunicazione (es. $c_i = DES_r(m$

[H] [width=0.8]RSAkey.png Schema RSA per Scambio Chiavi

Sicurezza e Uso Pratico di RSA

Padding: Non si deve mai usare RSA "puro" (textbook RSA). Se m è piccolo (es. $m^e < n$), un attaccante può calcolar

Lunghezza Chiave: La sicurezza dipende dalla grandezza di n. Oggi, chiavi n più corte di 1024 o 2048 bit non sono c

Efficienza: La generazione delle chiavi è lenta. La cifratura (con e piccolo) è veloce, la decifratura (con d grande) è len

Obiettivo Chiave usataOperazione