Schemi di cifratura a chiave publica

Rocco DE NICOLA
IMT Lucca
Rocco.DeNicola@imtlucca.it

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

Indice

- Introduzione
- Crittografia a doppia chiave
- Due breaktrough
  - Diffie-Hellman
  - RSA
- Attacchi e fattorizzazione

Crittografia a chiave simmetrica

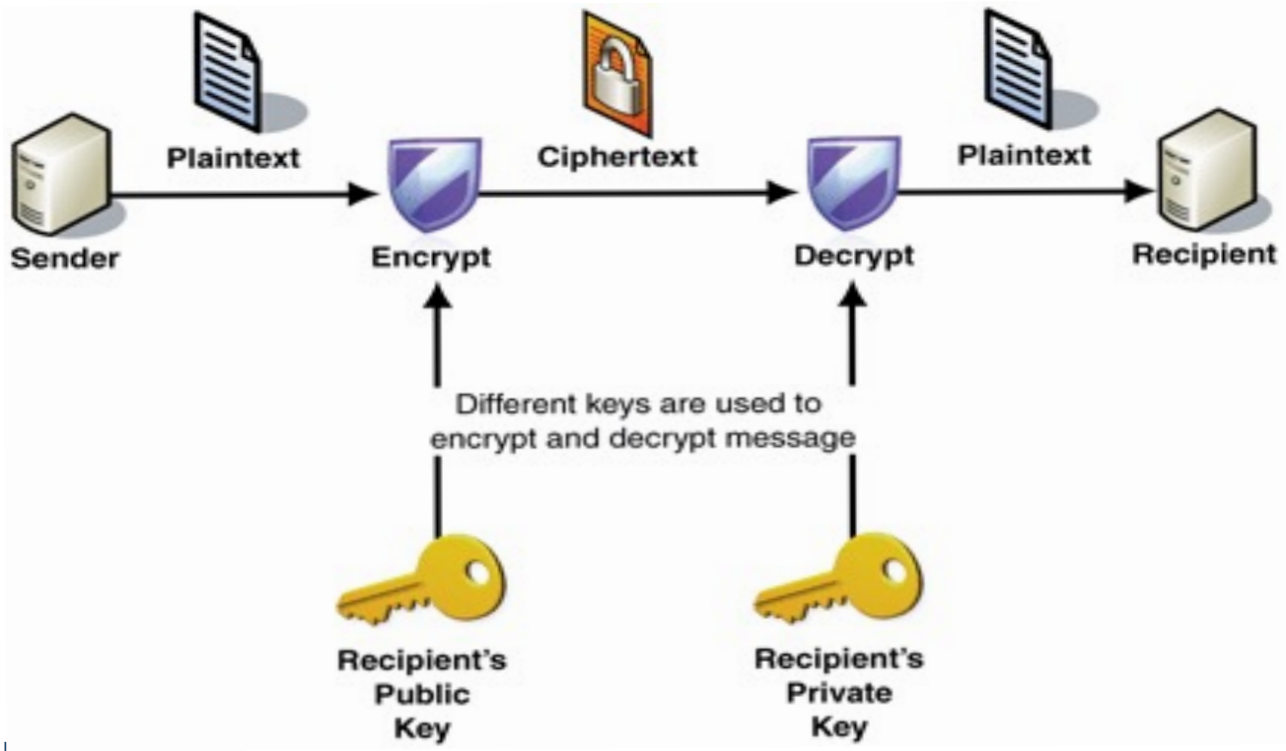
Gli schemi di cifratura (tradizionali) a chiave privata/segreta/singola:

- richiedono che il mittente e il destinatario abbiano ottenuto una copia della chiave segreta in modo sicuro e la tengano al sicuro.
- non proteggono il mittente da un destinatario che falsifica un messaggio e che poi asserisce che la richiesta è stata inviata dal mittente.

Crittografia a doppia chiave

- Gli schemi di cifratura (nuovi) a chiave pubblica / doppia / asimmetrica:
  - Prevedono l'uso di due chiavi:
    - una *chiave pubblica*, che può essere conosciuta da chiunque e che può essere utilizzata per cifrare i messaggi e verificare chi ha spedito
    - una corrispondente *chiave privata*, nota solo al destinatario, utilizzata per decifrare i messaggi e firmare
  - Realizzano uno scambio asimmetrico: la chiave usata per cifrare i messaggi o verifica le firme non può decifrare i messaggi o creare firme

Cifratura asimmetrica



Crittografia a doppia chiave

- Sviluppato per affrontare due problemi cruciali:
  - distribuzione delle chiavi: garantire comunicazioni sicure con una chiave personale senza dipendere da un centro distribuzione chiavi o fidarsi del comportamento di altri.
  - firme digitali: verificare che un messaggio provenga intatto dal mittente dichiarato
- Complementa piuttosto che sostituire la crittografia a chiave privata
- Si basa su proprietà garantite dalla teoria dei numeri piuttosto che sull'uso permutazioni e sostituzioni

Cifratura asimmetrica vs. cifratura simmetrica

Crittografia simmetrica

- Stesso algoritmo usato per cifrare e decifrare con la stessa chiave.
- Chiave e algoritmo sono condivisi da mittente e ricevente.
- La chiave deve essere tenuta segreta.
- Quasi impossibile decifrare un messaggio se si conoscono solo l'algoritmo e il testo cifrato.

Crittografia asimmetrica

- Stesso algoritmo usato per cifrare e decifrare cifrare ma si usano due chiavi: una per cifrare e una per decifrare.
- Mittente e ricevente devono avere ognuno una chiave che fa coppia con l'altra (non la stessa).
- Quasi impossibile decifrare un messaggio se si conoscono solo l'algoritmo, il testo cifrato e una delle chiavi (da una non si può risalire all'altra).

Gestione delle chiavi

- Ogni utente genera una coppia di chiavi da utilizzare per la cifratura e la decifratura dei messaggi:
  - La chiave pubblica viene inserita in un registro pubblico o in un altro file accessibile
  - La chiave "gemella" viene tenuta privata;
  - Ciascun utente mantiene una collezione di chiavi pubbliche di altri utenti
- Se Bob cifra un messaggio con la chiave pubblica di Alice, solo Alice potrà decifrarlo usando la propria chiave private (confidenzialità)
- Se Bob cripta il messaggio con la sua chiave privata, Alice e chi conosce la chiave pubblica di Bob potrà decifrarlo (autenticità)

Principali proposte

- D-H (Diffie-Hellman 1976): Primo algoritmo a chiave pubblica reso pubblico. Permette a due utenti di condividere un segreto da utilizzare come chiave per successive cifratura simmetrica dei messaggi
- RSA (Rivest, Shamir, Adleman 1977): L'approccio più usato per la crittografia a chiave pubblica
- ECC (Koblitz and Miller 1985) - Crittografia a curva ellittica proposta come alternativa a RSA, con lo stesso livello di sicurezza ma con chiavi molto più piccole
- DSS (U.S. NIST 1991) Standard di firma digitale rivisto spesso fino al 2013. Fornisce solo la funzione di firma digitale, non può essere utilizzato per cifrare o scambiare chiavi.

Principali proposte per PKC

Algorithm	Firma Digitale	Scambio di Chiave	Cifratura / Decifratura
Rivest, Shamir, Adleman (RSA)	Si	Si	Si
Diffie-Hellman (D-H)	No	Si	No
Digital Signature Standard (DSS)	Si	No	No
Elliptic Curve Cryptography (ECC)	Si	Si	Si

Requisiti per le funzioni crittografiche

- Computazionalmente:
  - poco costoso creare coppie di chiavi
  - poco costoso cifrare messaggi per il mittente che conosce la chiave pubblica e decifrare messaggi per il destinatario che conosce la chiave privata
  - difficile per un avversario scoprire la chiave privata conoscendo la chiave pubblica e decifrare un messaggio senza conoscere la chiave privata
- Possibile usare una qualunque delle due chiavi correlate per la cifratura e l'altra per la decifratura

Requisiti per le funzioni crittografiche/2

Gli schemi a chiave pubblica (PKC) dipendono da appropriate funzioni trap-door one-way

- Funzioni one-way
  - $Y = f(X)$ Facile!
  - $X = f^{-1}(Y)$ Difficile - non fattibile!
- Una funzione trap-door one-way deve essere tale che
  - $Y = f_k(X)$ è facile se k e X sono noti - encryption
  - $X = f_k^{-1}(Y)$ è facile se k e Y sono noti - decryption
  - $X = f_k^{-1}(Y)$ è non fattibile, se è noto solo Y

N.B. Un problema è facile se può essere risolto in tempo polinomiale in funzione della lunghezza dell'ingresso

Un esempio di funzione one-way

Dato il numero 6895601 stabilire se esso è il prodotto di due numeri primi, e quali sono questi numeri.

- Una soluzione naturale sarebbe quella di provare a dividere 6895601 per diversi numeri primi più piccoli del numero in considerazione fino a trovare la risposta.
- Ma se si sa che 1931 è uno dei numeri, si può trovare la risposta utilizzando una qualsiasi calcolatrice per calcolare 6895601 ÷ 1931

Attacchi

- Attacchi di forza bruta a PKC sono teoricamente possibili
- L'attacco è noto, ma, ricorrendo numeri molto grandi, la soluzione viene reso sufficientemente complesso perché sia impraticabile
- Vengono usare chiavi molto grandi: uno schema con chiave privata di 64 bit ha una sicurezza simile a quella garantita da una chiave di 512 bit in RSA

- N.B.: Chiavi più lunghe implicano che cifraturare e decifratura richiedono più tempo.

Teoria dei numeri

- La teoria dei numeri è fondamentale per affrontare le sfide della crittografia asimmetrica.
- Gli ingredienti basilari per lo sviluppo di una teoria della crittografia a doppia chiave sono:
  - I numeri primi
  - Aritmetica modulare
  - Esponenziazione e logaritmi

Due Breaktrough

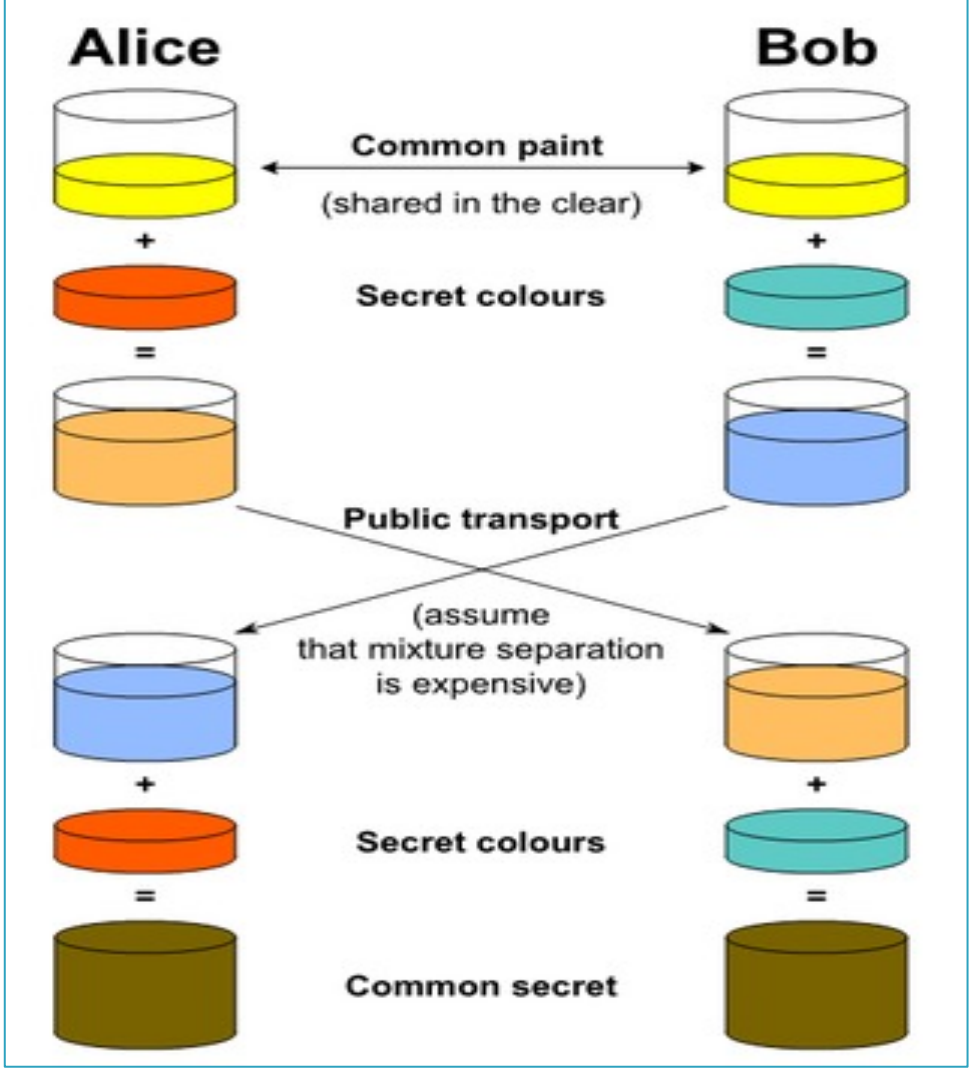
- Algoritmo per lo scambio di chiave (Diffie-Hellman-Merkle 1976):
  - L'algoritmo è stato progettato per consentire agli utenti di raggiungere un accordo sicuro su un segreto condiviso da utilizzare come chiave per le successive cifrature simmetriche.
  - Il brevetto USA 4.200.770 del 1977, ora scaduto, descrive l'algoritmo di dominio pubblico.
- Schema a chiave pubblica (RSA - Rivest, Shamir, Adleman 1977)
  - L'approccio più accettato e implementato di crittografia a chiave pubblica
  - la chiave di cifratura è pubblica e distinta dalla chiave di decifratura che è tenuta segreta (privata).

Diffie-Hellman

- L'algoritmo di Diffie-Hellman è un metodo per lo scambio sicuro di chiavi crittografiche su un canale pubblico ed è stato il primo protocollo a chiave pubblica ad essere reso noto.
- Tradizionalmente, la comunicazione criptata sicura tra due parti richiedeva che le chiavi venissero scambiate prima attraverso un qualche canale fisico (ad esempio un corriere di fiducia).
- Il metodo di scambio di chiavi Diffie-Hellman permette a due parti che non hanno alcuna conoscenza reciproca, di stabilire una chiave segreta condivisa su un canale non sicuro.
- Hellman ha suggerito di chiamare l'algoritmo Diffie-Hellman-Merkle

Diffie-Hellman Intuizione

Come ottenere un colore condiviso partendo da una vernice concordata e mantenendone due segrete.



Diffie-Hellman: matematicamente

- Alice e Bob si accordano su:
  - un numero primo q molto grande (1024 bit, circa 300 cifre decimali)
  - una radice primitiva g di q (più piccola di q)
- Alice sceglie numero segreto casuale a, calcola $g^a \bmod q$ e lo manda a Bob.
- Bob sceglie un numero segreto casuale b, e calcola $g^b \bmod q$ e lo manda ad Alice
- Con calcoli successive i due trovano lo stesso nymero
- $K_A = (g^b \bmod q)^a \bmod q = g^{ba} \bmod q = g^{ab} \bmod q$
  $= (g^a \bmod q)^b \bmod q = K_B$

Diffie-Hellman: un esempio

- Alice e Bob concordano di basarsi su un gruppo ciclico finito G di ordine n e sull'elemento generatore g in G (scelgono i primi p = 23 e g = 5).
- Alice sceglie un valore casuale a = 6, calcola A = 5^6 mod 23 (= 8) e lo invia a Bob insieme a 5 e 23.
- Bob sceglie un valore casuale b = 15, calcola B = mod 23 (= 19) lo invia ad Alice
- Con successivi calcoli i due ottengono la stessa chiave $K_A = K_B$
  - Alice calcola $K_A = 19^6$ mod 23 = 2
  - Bob calcola $K_B = 8^{15}$ mod 23 = 2
  - $K_B\ (g^a \text{ mod } p)^b \text{ mod } p = K_B$
- I segreti sono 6 (a), 15 (b) e soprattutto, 2 (g^{ab} e g^{ba})
- Eva (la cattiva) senza a e b, e con le sole A e B non può far nulla

RSA

- Basato sull'esponenziazione sugli interi modulo un numero primo - n
  - cifratura e decifratura sono singole esponenziazioni (mod n): l'esponenziazione è facile
  - la sicurezza garantita dal costo della difficile fattorizzazione di grandi numeri.
  - Vengono usati interi molto grandi (tipicamente 1024 bit)

RSA cifratura e decifratura

- Chiave Pubblica - PU = {e, n} - Chiave Privata - PR = {d, n}
- Per cifrare un messaggio M il mittente:
  - Usa la chiave **pubblica del destinatario** PU = {e,n}
  - Calcola $C = M^e \bmod n$, con $0 \leq M < n$
- Per decifrare C il destinatario:
  - usa la sua chiave privata PR = {d,n}
  - Calcola: $M = C^d \bmod n$
- La "magia" sta nella scelta del modulo e degli esponenti tali che

$$(M^e \bmod n)^d \bmod n = M$$

Generazione di chiavi con RSA

Ogni utente genera una coppia di chiavi pubbliche/private:

- Scegliendo casualmente due numeri primi : p, q
- Calcolando n = p X q e $\phi(n) = (p-1) X (q-1)$ (ϕ: totiente di Eulero)
- Scegliendo casualmente la chiave pubblica e tale che
  - $1 < e < \phi(n)$ con e e $\phi(n)$ coprimi ($gcd(e, \phi(n))=1$)
- Determina la chiave privata d risolvendo l'equazione
  - $(e \times d) \bmod \phi(n) = 1$ with $0 \leq d \leq n$
- Pubblica la chiave pubblica (PU={e,n}) e tiene segreta la chiave privata (PR={d,n}).

Attacchi

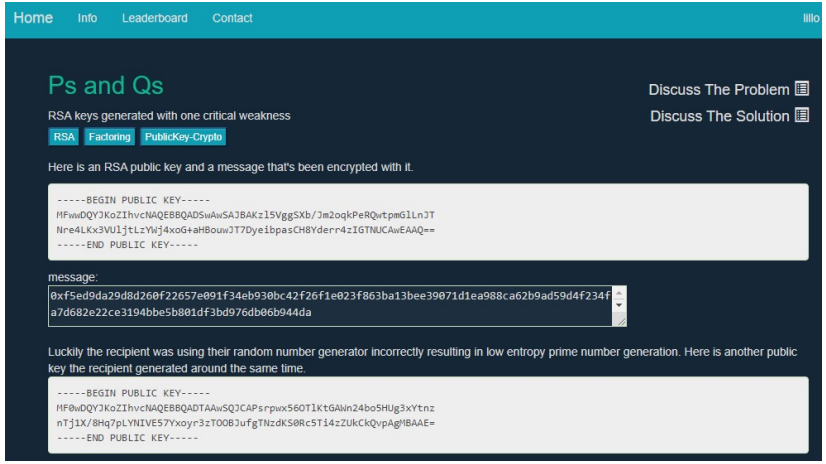
- Attacchi di forza bruta sono teoricamente possibile
- Il problema è noto, ma è reso sufficientemente difficile da renderne la risoluzione impraticabile
- Richiede l'utilizzo di numeri molto grandi

Attacchi di forza bruta a RSA

Con chiavi corte, il modulo può essere fattorizzato con attacchi di forza bruta.

- Un modulo a 256 bit può essere calcolato in un paio di minuti.
- Un modulo a 512 bit richiede diverse settimane per l'hardware di consumo moderno.
- La fattorizzazione di chiavi a 1024 bit non è sicuramente possibile in un tempo ragionevole con mezzi ragionevoli, ma può essere possibile per attaccanti ben equipaggiati.
- Il modulo a 2048 bit è sicuro contro attacchi alla fattorizzazione con forza bruta.
- I computer quantistici potrebbero cambiare lo scenario: " *How to factor 2048 bit RSA Integers in 8 Hours using 20 million noisy qubits*" (arxiv.org/abs/1905.09749)

Esempio di attacco a RSA



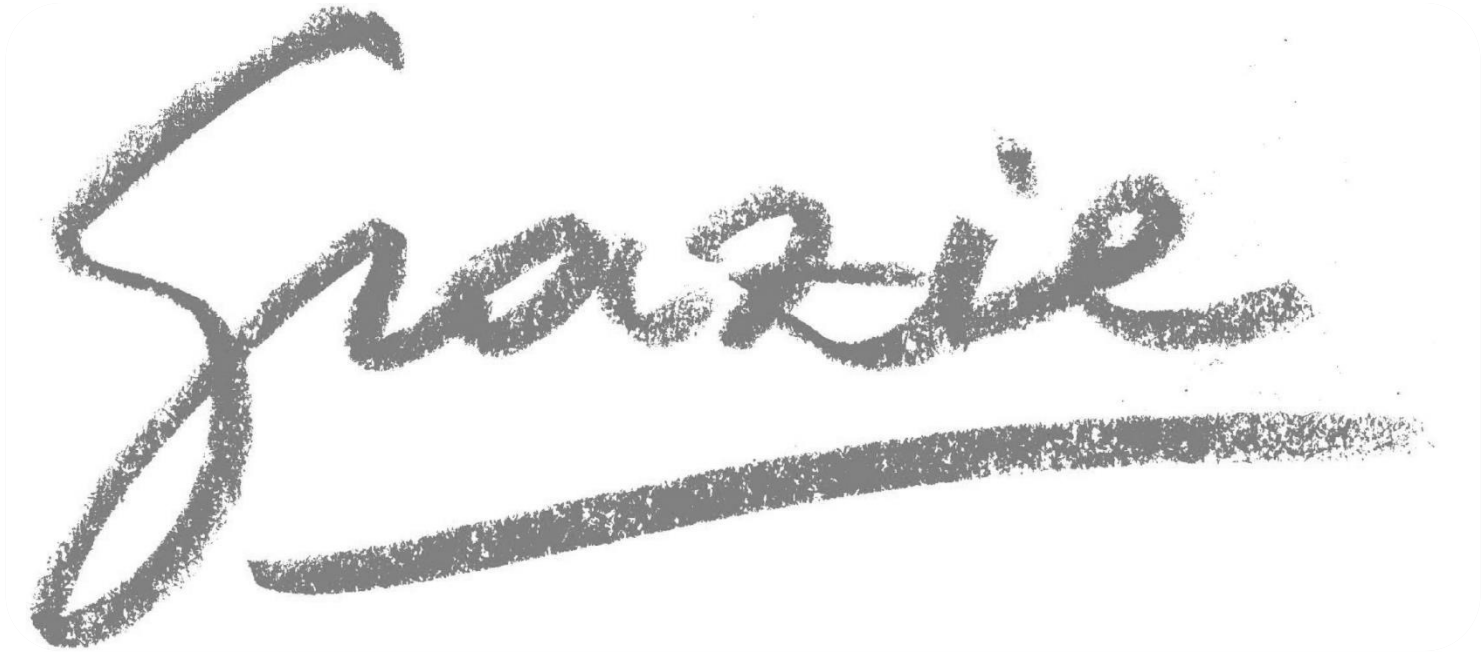
https://id0-rsa.pub/problem/8/

```python
import gmpy2
from Crypto.PublicKey import RSA

c = 0xf5ed9da29d8d260f22657e091f34eb930bc42f26f1e023f863ba13bee39071d1ea988ca62b9ad59d4f234fa7d682
e22ce3194bbe5b801df3bd976db06b944da

pem1 = """-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKzl5VggSXb/Jm2oqkPeRQwtpmGlLnJT
Nre4LKx3VUljtLzYWj4xoG+aHBouwJT7DyeibpasCH8Yderr4zIGTNUCAwEAAQ==
-----END PUBLIC KEY-----"""

pem2 = """-----BEGIN PUBLIC KEY-----
MF0wDQYJKoZIhvcNAQEBBQADTAAwSQJCAPsrpwx56OTlKtGAWn24bo5HUg3xYtnz
nTj1X/8Hq7pLYNIVE57Yxoyr3zTOOBJufgTNzdKS0Rc5Ti4zZUkCkQvpAgMBAAE=
-----END PUBLIC KEY-----"""


key1, key2 = RSA.importKey(pem1), RSA.importKey(pem2)

p = gmpy2.gcd(key1.n, key2.n)
q1 = key1.n // p
phi_n1 = (p-1)*(q1-1)
d = gmpy2.invert(key1.e, phi_n1)
m = pow(c, d, key1.n)
print('{:x}'.format(m))
```

Nota: l'attacco è possibile perché un numero primo P usato per generare il modulo di una chiave è usato per generare il modulo di un'altra

Idee sbagliate

- La crittografia a chiave pubblica è più resistente ad attacchi di crittoanalisi della crittografia simmetrica
  - Non c'è nulla in linea di principio che renda l'una superiore all'altra dal punto di vista della resistenza alla crittoanalisi
- La crittografia a chiave pubblica ha reso obsoleta la crittografia simmetrica
  - L'overhead computazionale della crittografia a chiave pubblica suggerisce che la crittografia simmetrica non sarà abbandonata
- La distribuzione delle chiavi è banale per la crittografia a chiave pubblica, mentre l`uso di centri di distribuzione delle chiavi per la crittografia simmetrica è pesante
  - Anche per la cifratura a chiave pubblica, sono necessary protocolli che spesso coinvolgono un agente centrale, e le procedure non sono più semplici.



Schemi di cifratura a chiave publica

Rocco DE NICOLA
IMT Lucca
Rocco.DeNicola@imtlucca.it

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it