

# Standard di crittografia pubblica: RSA

Lezione 5 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)  
Facoltà di Scienze Matematiche, Fisiche e Naturali  
Corso di Studi in Informatica applicata, AA 2006-7

## Indice

1. Standard di crittografia pubblica: RSA
2. crittografia a chiave pubblica: RSA
3. validità di RSA
4. confronto fra crittografia simmetrica e asimmetrica
5. riferimenti

## crittografia a chiave pubblica: RSA

**RSA**, dalle iniziali dei nomi degli inventori: **Rivest, Shamir, Adelman (1978)**  
come funziona (essenzialmente):

una coppia di chiavi associate è costituita da due coppie  $(n, e)$ ,  $(n, d)$ , tali che, per qualsiasi testo in chiaro  $M$ , considerato come numero binario naturale:  
 $(M^e)^d = (M^d)^e = M \pmod{n}$

si scelgono  $n$ ,  $e$ ,  $d$  tali da soddisfare le seguenti proprietà:

$n = pq$ , con  $p$ ,  $q$  primi molto grandi (256 bit o più), dunque  $\varphi(n) = (p-1)(q-1)$

$e$  primo relativo con  $\varphi(n)$ , cioè  $\gcd(e, \varphi(n)) = 1$

$d$  inverso di  $e \pmod{\varphi(n)}$ , cioè  $ed = 1 \pmod{\varphi(n)}$  (\*)

Teorema di Eulero:  $M^{\varphi(n)} = 1 \pmod{n}$ , se  $M$ ,  $n$  primi relativi

se  $M$ ,  $n$  sono primi relativi, lo sono sia  $M$ ,  $p$  che  $M$ ,  $q$ , dunque:

$M^{p-1} = 1 \pmod{p}$ ,  $M^{q-1} = 1 \pmod{q}$ , e per  $k$  tale che  $ed = k\varphi(n) + 1$  (tale  $k$  esiste per la proprietà (\*)), elevando entrambi i membri della prima equazione a  $k(q-1)$  e quelli della seconda equazione a  $k(p-1)$ , si ottiene:

$M^{k\varphi(n)} = 1 \pmod{p}$ ,  $M^{k\varphi(n)} = 1 \pmod{q}$ , donde  $M^{k\varphi(n)} = 1 \pmod{n}$

e quindi, moltiplicando ambo i membri per  $M$ :  $M^{ed} = M \pmod{n}$

## validità di RSA

come altri algoritmi di crittografia a chiave pubblica (Diffie-Hellman (1976), Merkle-Hellman (1978), Elgamal (1985)), RSA è basato su un problema computazionalmente **difficile**, in questo caso:

**determinazione dei fattori primi** di un dato numero (abbastanza grande)

la complessità del problema del **test di primalità** è stata recentemente provata essere **polinomiale**, con l'AKS Primality Test (Agrawal, Kayal & Saxena, 2002)

... tuttavia ciò non invalida la crittografia RSA perché nessun algoritmo polinomiale è noto per il problema della **fattorizzazione in primi**

RSA soddisfa i tre criteri di validità per sistemi di crittografia commerciale, ma non è esente da **minacce**:

si è già rivelata fattibile la fattorizzazione del numero **RSA-200**; rimane aperta quella dei numeri più grandi della RSA Factoring Challenge

algoritmi **quantistici** (probabilistici) per il problema della fattorizzazione, e per altri di simile difficoltà, hanno complessità polinomiale, v. (Shor, 1995): ciò potrebbe minacciare la validità di RSA con tecnologie future

## confronto fra crittografia simmetrica e asimmetrica

le radicalmente differenti caratteristiche di **riservatezza delle chiavi** e la notevolmente diversa **velocità degli algoritmi** di cifratura e decifrazione comportano usi diversi, ma spesso **complementari**, della crittografia simmetrica e di quella asimmetrica

| caratteristica             | crittografia simmetrica   | crittografia asimmetrica                                      |
|----------------------------|---|---|
| numero di chiavi           | 1   | 2   |
| riservatezza delle chiavi  | segreta, condivisa  | una chiave pubblica, l'altra segreta (locale)                 |
| velocità dell'algoritmo    | rapida  | più lenta, per un fattore $\sim 10^4$                         |
| distribuzione della chiave | singolarmente per ciascun canale                                    | si può usare la chiave pubblica per distribuire altre chiavi  |
| usi migliori               | uso estensivo della crittografia, riservatezza e integrità dei dati | crittografia una tantum, scambio delle chiavi, autenticazione |

## riferimenti

**Rivest, Shamir, Adelman (1978) :**

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,  
Comm. ACM 21, 120-126, 1978. <http://theory.csail.mit.edu/~rivest/publications.html>

**Diffie & Hellman (1976) :** New Directions in Cryptography,

IEEE Trans. on Info. Theory, IT-22(6), 644-654, 1976.  
<http://www-ee.stanford.edu/~hellman/publications.html>

**Merkle & Hellman (1978) :** Hiding Information and Signatures in Trapdoor Knapsacks,

IEEE Trans. on Info. Theory, IT-24(5), 525-536, 1978.  
<http://www-ee.stanford.edu/~hellman/publications.html>

**Elgamal (1984) :** A public key cryptosystem and a signature scheme based on discrete logarithms,

in: Advances in Cryptology: Proc. CRYPTO 84, LNCS 196(4), 10-19, Springer, 1985.  
<http://www.springerlink.com/content/cemajg0qmeev>

**Agrawal, Kayal & Saxena (2002) :** PRIMES is in P, Annals of Mathematics, 160(2): 781-793, 2004.

<http://www.cse.iitk.ac.in/users/manindra/publications.html>

**AKS Primality Test :** <http://mathworld.wolfram.com/AKSPrimalityTest.html>

**RSA Factoring Challenge :** <http://www.rsa.com/rsalabs/node.asp?id=2092>

**Shor (1995) :**

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,  
SIAM J. Computing, 26 1484-1509, 1997. <http://www.arxiv.org/abs/quant-ph/9508027>