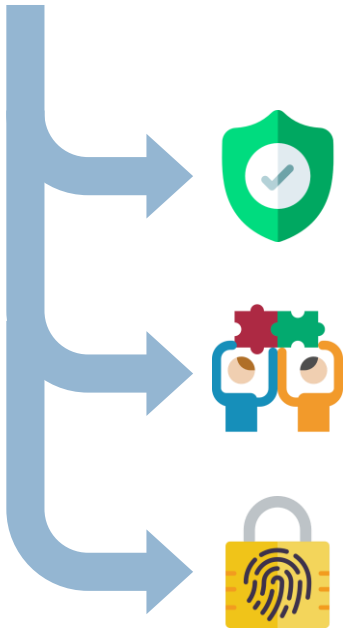
Crittografia RSA

FALAPPA Carlo, **CARLETTI** Mattia, **SIDERI** Michael, **LORENZETTI** Filippo e **PAPARELLI** Riccardo

Crittografia MODERNA

La **CRITTOGRAFIA MODERNA** nasce negli anni ‘70 con la scoperta dei primi algoritmi asimmetrici. Possiede tre prerogative:



RISERVATEZZA: l'informazione deve essere intelligibile solo da chi ne è autorizzato;

INTEGRITÀ: deve essere possibile rilevare se l'informazione è stata alterata;

AUTENTICAZIONE: la parte autenticarsi deve dimostrare alla parte autenticante chi sostiene di essere;

Crittografia ASIMMETRICA

Si dicono ALGORITMI **ASIMMETRICI** quelli che si basano su una **coppia di chiavi**: una capace di cifrare e l'altra di decifrare l'informazione.

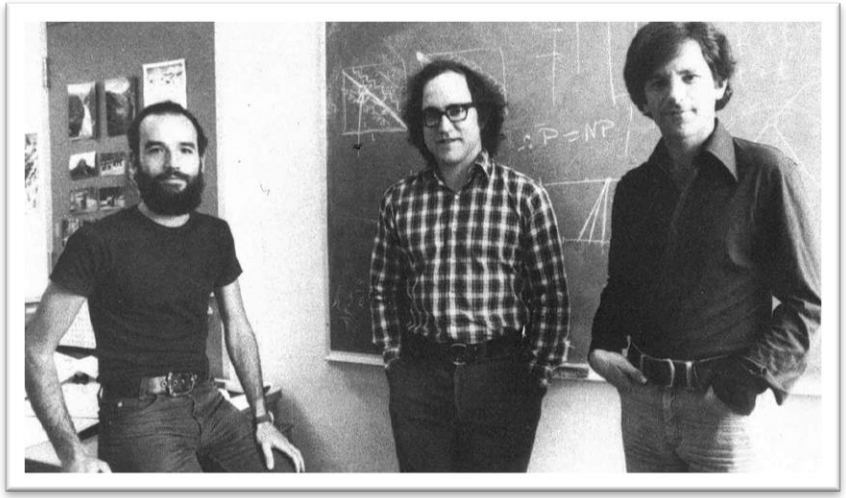
Utilizzando questa tipologia di algoritmo è possibile **distribuire la chiave crittazione** cosi da evitare il problema dello scambio di chiavi e mantenere segreta la chiave di decrittazione.

Crittografia RSA

Nato nel 1977, segna un punto importante nella storia della **Crittografia**, sostituendo i vecchi sistemi simmetrici con quelli asimmetrici. Si tratta di un cifrario a chiave pubblica che permette di cifrare un messaggio attraverso un procedimento che sfrutta le proprietà dei numeri primi.

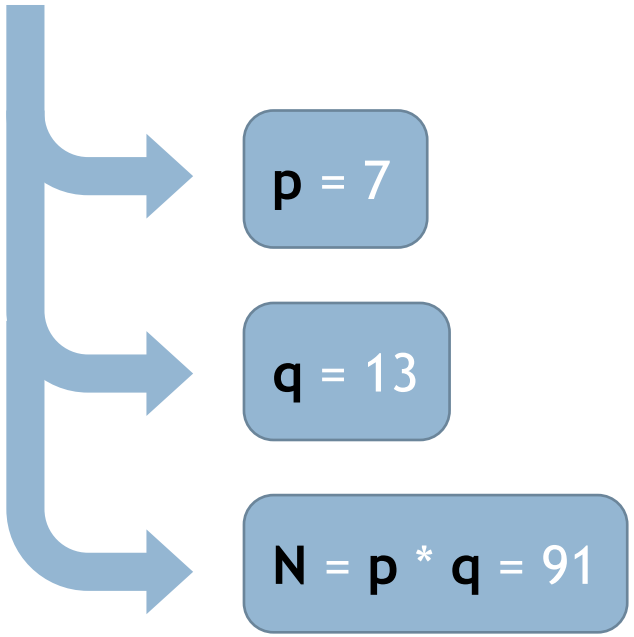
Il nome **R.S.A.** è l'acronimo dei nomi degli inventori:

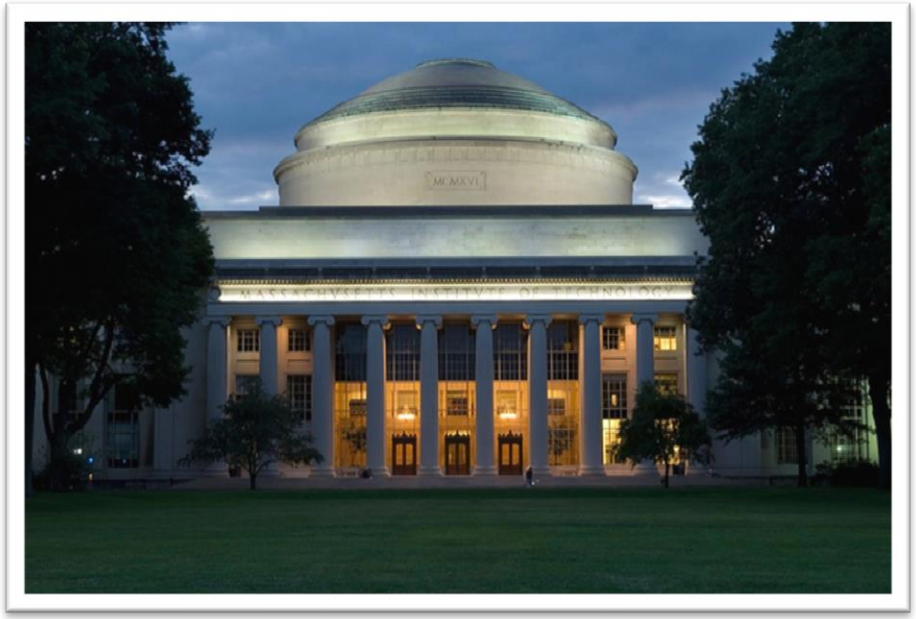
- Ronald **R**ivest (2);
- Adi **S**hamir (1);
- Leonard **A**dleman (3);



Metodo di CIFRATURA

Inizialmente bisogna considerare **due numeri primi distinti**, p e q, e moltiplicarli tra di loro ottenendo il numero N che viene reso pubblico, mentre i due numeri iniziali rimangono privati.





Metodo di CIFRATURA

Ora si deve calcolare il numero b tramite la **FUNZIONE DI EULERO**, b = Φ(N) = (p - 1) * (q - 1), che rimane segreto.

b = (p-1)*(q-1) = (7-1) * (13-1) = 72

Adesso si calcola il numero e che è il **PRIMO INTERO PRIMO CON b**, non abbia divisori in comune, ovvero MCD(e, b) = 1. Il numero e è la seconda chiave pubblica.

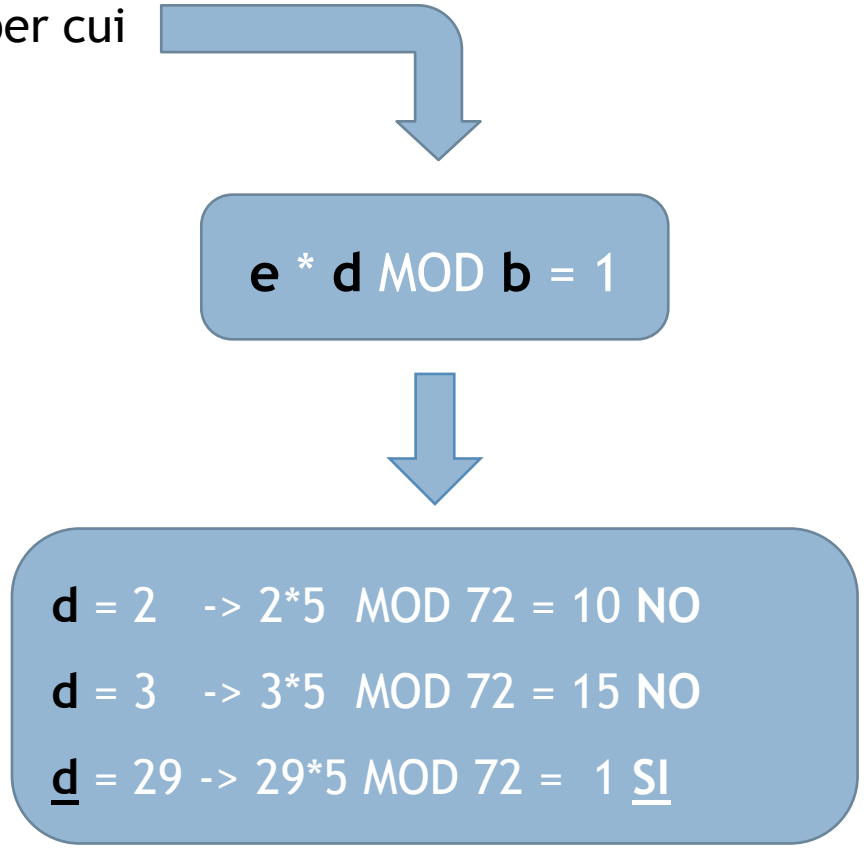
b = 72

e = 4 → MCD(4,72) = 2 --> NO

e = 5 → MCD(5,72) = 1 --> SI

Metodo di CIFRATURA

Il **NUMERO d** è la chiave che si utilizza per **decifrare** e deve restare segreto. Il numero **d** che è il numero più piccolo per cui



Metodo di CIFRATURA

Per poter trasmettere il messaggio, in accordo con il ricevente, si scegli un **metodo di traduzione** delle lettere in numeri: un metodo molto banale, potrebbe essere il far corrispondere le lettere al loro numero di posizione nell'alfabeto (A = 1, B = 2 ecc…). Utilizzando le chiavi pubbliche N e e, si trasmettono una alla volta i numeri m, ottenuti precedentemente, attraverso la formula $c = m^e \text{ MOD } N$.

Es.

Ciao = $3\hat{}(m_1)$ $9\hat{}(m_2)$ $1\hat{}(m_3)$ $15\hat{}(m_4)$

$c_1 = m_1^e \text{ MOD } N = 3^5 \text{ MOD } 91 = \underline{61}$

$c_2 = m_2^e \text{ MOD } N = 9^5 \text{ MOD } 91 = \underline{81}$

$c_3 = m_3^e \text{ MOD } N = 1^5 \text{ MOD } 91 = \underline{1}$

$c_4 = m_4^e \text{ MOD } N = 15^5 \text{ MOD } 91 = \underline{71}$

Metodo di DECIFRAZIONE

Per la decifrazione si utilizza il **NUMERO SEGRETO d** che permette di trovare i numeri m attraverso la **formula**:

$m = c^d \text{ MOD } N$

Messaggio **CIFRATO**: 61(c_1) 81(c_2) 1(c_3) 71(c_4)

$m_1 = c_1^d \text{ MOD } N \dashrightarrow 61^{29} \text{ MOD } 91 = 3$

$m_2 = c_2^d \text{ MOD } N \dashrightarrow 81^{29} \text{ MOD } 91 = 9$

$m_3 = c_3^d \text{ MOD } N \dashrightarrow 1^{29} \text{ MOD } 91 = 1$

$m_4 = c_4^d \text{ MOD } N \dashrightarrow 71^{29} \text{ MOD } 91 = 15$

FONTI

Università degli Studi di SALERNO

Università degli Studi di ROMA «Tor Vergata»

Crittografia.EU