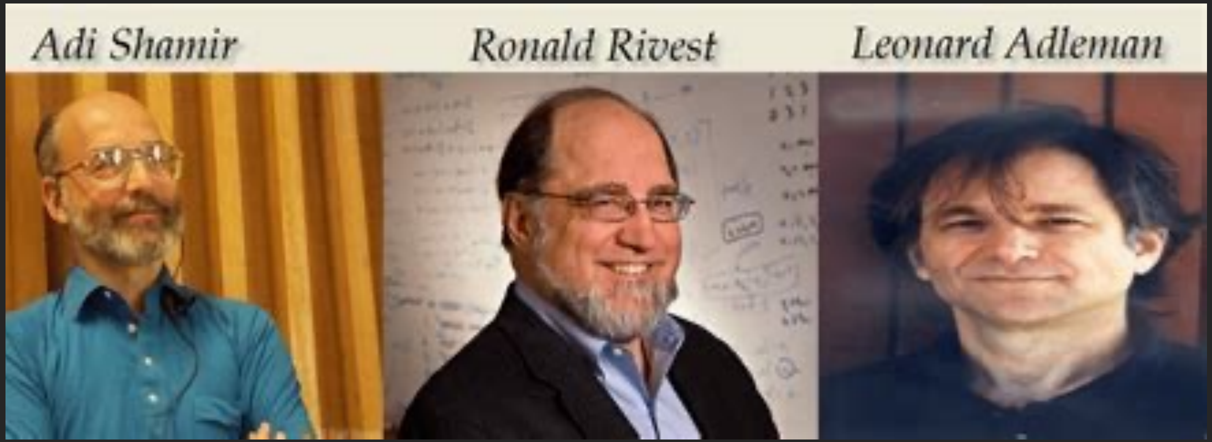
RSA Encryption

RSA



- Most popular function in public key cryptography
  - Invented in 1977 by Rivest, Shamir, and Adleman
  - Widely used in internet protocol like TLS, PKI

Textbook RSA scheme

- Three Algorithms (Gen, Enc, Dec)
  - Gen: on input a security parameter λ.
    - Generate two distinct primes p and q of same bit-size λ
    - Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$
    - Choose at random an integer e $(1 < e < \phi(N))$ such that $\gcd\big(e, \phi(N)\big) = 1$
    - Let $\mathbb{Z}_N^*$={x | 0 <x<N and gcd(x,N)=1}
    - Compute d such that $e \cdot d \equiv 1 \ (mod\ \phi(N))$
    - Public key $PK = (e, N)$. The private key $SK = e, d, N$

Textbook RSA scheme

- $Enc(PK, m)$: On input an element $m \in \mathbb{Z}_N^*$ and the public key $PK = (e, N)$ compute
  - $c = m^e \ (mod\ N)$
- $Dec(SK, c)$: On input an element $c \in \mathbb{Z}_N^*$ and the private key $SK = (e, d, N)$ compute
  - $m = c^d \ (mod\ N)$

Example

Generate two distinct primes p and q of same bit-size λ

Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$

Choose at random an integer e $(1 < e < \phi(N))$ such that $\gcd(e, \phi(N)) = 1$

Compute d such that $e \cdot d \equiv 1 \ (mod\ \phi(N))$

Public key $PK = (e, N)$. The private key $SK = e, d, N$

- $p = 3, q = 11$
- $N = 33, \phi(N) = 2 \cdot 10 = 20$
- Let $e = 7$
  - Note $\gcd(7{,}20) = 1$
- We find $d = 3$ as
  $7 \cdot 3 + (-1) \cdot 20 = 1$
- $PK = (e = 7, N = 33)$
- $SK = (e = 7, d = 3, N = 33)$

Example

- $Enc(PK, m)$: On input an element $m \in \mathbb{Z}_N^*$ and the public key $PK = (e, N)$ compute
  - $c = m^e \ (mod\ N)$
- $Dec(SK, c)$: On input an element $c \in \mathbb{Z}_N^*$ and the private key S$K = (e, d, N)$ compute
  - $m = c^d \ (mod\ N)$

- $\mathbb{Z}_N^* = \{1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32\}$
- Let $m = 4$
- $c = m^e \ (mod\ N) = 4^7 \ (mod\ 33) = 16\ (mod\ 33)$
- We recover $m = c^d \ (mod\ N)$
  - $m = c^d \ (mod\ N) = 16^3 \ (mod\ 33) = 4\ (mod\ 33)$