RSA Encryption - Public Key Cryptosystem

Anyone can use Bob's public key to encrypt a message.

Bob posts his public key, and Bob keeps a secret key. This allows him to decrypt, but no one can either (a) figure out secret key or (b) decrypt msg using the public key.

One-way function is easy to compute but hard to reverse.

Ron Rivest - MIT prof
Adi Shamir - ?
Leonard Adleman - retired USC

Dec 76 – 1977

British Security Agency (equiv NSA in US)

71 or 72 a new hire Clifford Cocks (young) Participant in the International Math Olympiad.
In 3 weeks, Clifford came up with

2. Difffer-Hellman Key Exchange (KNI)
3. RSA

-1997 work declassified
Pick 2 large primes: \( p, q \) (Private keys)

1st public key is \( n = pq \) (factoring is hard)

Next we calculate \( \phi(n) = (p-1)(q-1) \) (This is private)

Pick random value \( e \) such that \( \gcd(e, \phi(n)) = 1 \).

Post \( e \) as the 2nd Public key.

Use Ext. Euclid Alg to solve for

\[ d = e^{-1} \mod \phi(n) \]

\( d \) is the Private key

Note: Given \( n, \phi(n) \), we can calculate \( p, q \)

\[ n = 7 \times 13 = 91 \]

\[ \phi(n) = 6 \times 12 = 72 \]

\[ pq = 91 \]

\[ (p-1)(q-1) = 72 \]

\[ pq - p - q + 1 = 72 \]

\[ 91 - p - q + 1 = 72 \]

\[ p + q = 20 \]

\[ q = 20 - p \]

Public keys: \( n, e \) \quad ed = 1 \mod \phi(n)

Private key: \( d \) \quad (always true)

To send a message \( M \) to Bob: Calculate \( C = M^e \mod n \).

To decrypt: Bob computes \( M = C^d \mod n \).
\[ C = M^e \mod n \]

\[(M^e)^d = M^{ed} \mod n \]
\[= M^{x \phi(n) + 1} \]
\[= M \cdot M^{\phi(n)} \]
\[= (M^{\phi(n)})x \cdot M \]
\[= 1 \cdot M \]
\[= M \mod n \]

\[ \text{Eve knows } n, e, \]
\[ \text{Eve knows } C = M^e \]

\[ \Rightarrow \text{She can't find } \phi(n). \]
\[ \Rightarrow \text{She can't find } d \equiv e^{-1} \mod \phi(n). \]
\[ \Rightarrow \text{Can't undo } C \text{ in another way}. \]

Key Size must be pretty big

\( \Rightarrow \text{ECC uses bit key RSA 2048 bit key} \)

\[ p = 17, \quad q = 23 \quad n = 391 \]
\[ \phi(n) = (p-1)(q-1) = (6 \times 22) = 352 = 2^3 \times 11 \]

Pick \( e \) s.t. \( \gcd(e, 352) = 1 \), \( e = 35 \)

Find \( d \).

\[ 352 = 10 \times 35 + 2 \]
\[ 35 = 17 \times 2 + 1 \]
\[ 35 - 17 \times 2 = 1 \]
\[ 35 - 17 \left(352 - 10 \times 35\right) = 1 \]
\[ 35 - 17 \times 352 + 170 \times 35 = 1 \]
\[ 171 \times 35 - 17 \times 352 = 1 \mod 352 \]
\[ d \equiv 171 \mod 391 \]

\[ C = 22 \mod 391 \]
\[ M = 0 \mod 391 \]