10/30/19 (1)

RSA Encryption - Public Key Cryptosystem

Anyone $\xrightarrow[\text{to encrypt msg.}]{\text{use Bob's public key}}$ Bob posts his Public Key

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

One-way function

$\xrightarrow{\quad\quad\quad}$
easy

$\xleftarrow{\quad\quad\quad}$
hard

Ron Rivest - MIT prof
Adi Shamir - ?
Leonard Adleman - retired USC
early 70s
Dec ~~'7~~ '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
<u>BOTH</u> (2) Diffie-Hellman Key Exchange AND
(1) RSA
-1997 Work Declassified

10/30/19

Pick 2 large primes: p, q. (Private keys)

1^{st} 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 2^{nd} Public key.

Use Ext. Euclid Alg to solve for

$d \equiv e^{-1} \mod \phi(n)$.

Technically $p, q, \phi(n)$ are not keys, but they MUST remain private.

$\boxed{d \text{ is the Private key}}$

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

$n = 7 \times 13 = 91$

$\phi(n) = 6 \times 12 = 72$

$pq = 91$

$(p-1)(q-1) = 72$

$pq - p - q + 1 = 72$

$91 - p - q + 1 = 72$

$\boxed{p + q = 20} \longrightarrow \boxed{q = 20 - p}$

$p(20-p) = 91$

$20p - p^2 = 91$

$\boxed{p^2 - 20p + 91 = 0}$

Quadratic

Public keys: n, e

Private key: d

, $ed \equiv 1 \mod \phi(n)$

(always true)

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

To decrypt Bob Computes $M = C^d \mod n$.

10/30/19 (3)

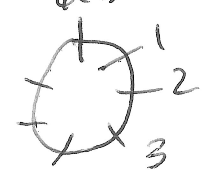
$$C = M^e \mod n$$

$$(M^e)^d \equiv M^{ed}$$
$$\equiv M^{x\phi(n)+1}$$
$$\equiv M^{\phi(n)x} \cdot M^1$$
$$\equiv (M^{\phi(n)})^x \cdot M^1$$
$$\equiv 1^x \cdot M^1$$
$$\equiv M \mod n$$

$ed \equiv 1 \mod \phi(n)$
$\hookrightarrow \exists x \in \mathbb{Z}$ s.t. $\boxed{ed = x\phi(n)+1}$

assume $\gcd(M,n)=1$.
$\hookrightarrow$ prob this isn't the case is very small.

$$M^{\phi(n)} \equiv 1 \pmod{n}$$



Eve knows n, e.
Eve knows $C = M^e$
$\hookrightarrow$ She can't find $\phi(n)$.
She can't find $d \equiv e^{-1} \mod \phi(n)$.
Can't UNDO "e" in another way.

Key size must be pretty big
$\hookrightarrow$ ECC 400 bit key RSA 2048 bit key

$$p = 17, \quad q = 23 \qquad n = 391$$

$$\phi(n) = (p-1)(q-1) = 16 \times 22 = 352 = 2^2 \times 2^3 \times 11$$

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

Find d.

32
32
88
$4 | 352$

$352 = 10 \times 35 + 2$
$35 = 17 \times 2 + 1$
$35 - 17 \times 2 = 1$
$35 - 17(352 - 10 \times 35) = 1$
$35 - 17 \times 352 + 170 \times 35 = 1$
$171 \times 35 - 17 \times 352 \equiv 1 \mod 352$
$d \equiv 171 \mod 352$

$M = 22$
$C = 22^{35} \mod 391$
$M = \bigcirc^{171} \mod 391$

RSABigInt.java

RSA2BigInt.java