The Rivest Shamir Adelman (RSA) Public Key Cryptosystem

What is public-key cryptography?

$$\boxed{A} \xleftrightarrow{\text{communications}} \boxed{B}$$

Public Key crytography

$$\boxed{A} \xrightarrow{\text{encrypt message using public info}} \boxed{B}$$

only B can read it.

RSA

Choose primes p and q (typically very large) but we use $p = 7$ and $q = 13$.

Lemma: $\phi(pq) = (p-1)(q-1)$

$\varphi(pq) = |U(pq)| = \#$ of residue classes mod pq that are not divisible by p or q.

Proof. $p = 5 \quad q = 7$

35 classes.

$\cancel{0}, 1, 2, 3, 4, \cancel{5}, 6, 7, \ldots$

7 are multiples of 5.

5 multiples of 7.

35 − 7 multiples of 5 − 5 multiples of 7 + 1

$35 - 7 - 5 + 1 = (7-1)(5-1)$
$= 6 \cdot 4 = 24.$

pq: 0 once

$1\cdot p, 2\cdot p, \ldots (q-1)p = q-1$ multiples of p

$1\cdot q \ldots\ldots (p-1)q = p-1$ multiples of q

\# multiples of p or $q = 1 + q - 1 + p - 1$
$= q + p - 1$

Left over: $pq - (p+q-1) = pq - p - q + 1$
$= (p-1)(q-1).$

Let $m = (p-1)(q-1)$. Pick D relatively prime to m and solve $DE \equiv 1 \pmod{m}$.

$p = 7 \quad q = 13$

$m = 6 \cdot 12 = 72$

- $m = 72$
- $D = 5$ ✓
- $E = 29$.

$DE \equiv 1 \mod 72$

$5 \cdot 29 = 145 = 2 \cdot 72 + 1$

$DE \equiv 1 \mod 72.$

By Euler's Theorem, $(x^D)^E = x^{DE} \equiv \cancel{1}\, x \pmod{N}$.

$x \mod N$
Not div by p, q.

$$(x^D)^E \equiv x^{DE} \equiv x^{1+km}$$
$$\equiv x \cdot \left(\underline{x^{\varphi(N)}}\right)^k$$
$$\equiv x \mod N.$$

$DE \equiv 1 \mod m$

$m = \varphi(N)$

Publish E and N. Hide D and $\cancel{D}$. m

- E is called the encryption key or the public key.
- D is called the decryption key or the private key.

$N = 91, \quad E = 29$

$D = 5 \quad \cancel{m = 72}$

Example

$N = 91$ and $E = 29$. Secret message is 19. Compute

$\boxed{A} \xrightarrow{80} \boxed{B}$

$N, 29$ $D\ (N)$

E

$$19^E \equiv 19^{29} \equiv 80 \pmod{91}$$

$19^{29} \bmod N \equiv 80 \bmod 91$

Send 80 to the recipient.

Recipient computes

$80^5 \equiv 19 \pmod{91}$

$$80^5 \equiv 19 \pmod{91}$$

to recover the message

Security

Given E and N, to find D and m you need to find $(p-1)(q-1)$, which means you need to find p and q, which means you need to factor N.

If N is large this is impractical. Typically N several hundred digits.

Conceivable that quantum computers will make this insecure.

$\longrightarrow DE \equiv 1 \bmod m$

Given $N = pq$, can you find $(p-1)(q-1) = m$?

$N \sim 600$ digits

$E, D \sim 600$ digits

$x^E \bmod N.$