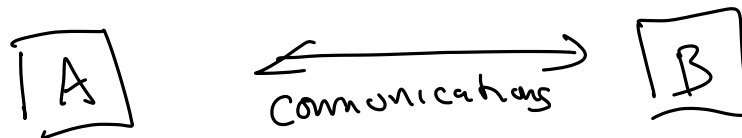
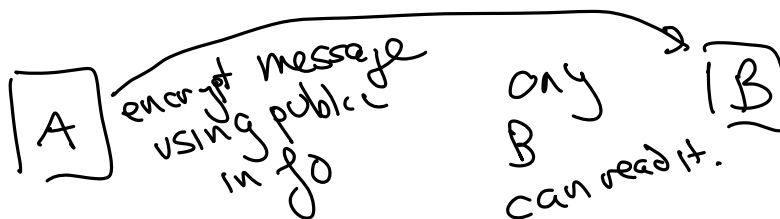


The Rivest Shamir Adelman (RSA) Public Key Cryptosystem

What is public-key cryptography?



Public Key cryptography



RSA

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

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

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

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

$\emptyset, 1, 2, 3, 4, \cancel{5}, 6, 7, \dots$

$35 - 7$ multiples of $5 - 5$ multiples of $7 + 1$

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

35 classes.
7 are multiples of 5.
5 multiples of 7.

pq : 0 once

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

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

$$\begin{aligned} \# \text{ multiples of } p \text{ or } q &= 1 + q - 1 + p - 1 \\ &= q + p - 1 \end{aligned}$$

$$\begin{aligned} \text{left over: } pq - (p + q - 1) &= pq - p - q + 1 \\ &= (p-1)(q-1). \end{aligned}$$

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

$$p = 7 \quad q = 13 \\ m = 6 \cdot 12 = 72$$

- $m = 72$
- $D = 5$ ✓
- $E = 29$.

$$DE \equiv 1 \pmod{72} \\ 5 \cdot 29 = 145 = 2 \cdot 72 + 1 \\ DE \equiv 1 \pmod{72}$$

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

$$\begin{aligned} (x^D)^E &\equiv x^{DE} \equiv x^{1+km} \\ &\equiv x \cdot \underbrace{(x^{\varphi(N)})^k} \\ &\equiv x \pmod{N}. \end{aligned}$$

$x \pmod{N}$
not div by p, q .

$$DE \equiv 1 \pmod{m} \\ m = \varphi(N)$$

Publish E and N . Hide D and ~~m~~ .

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

$$N = 91, \quad E = 29$$

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

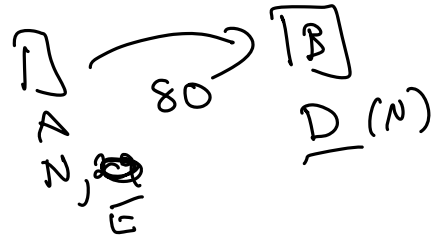
Example

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

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

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

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.

$$\rightarrow DE \equiv 1 \pmod{m}$$

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

$N \sim 600$ digits

BRAGAO $E, D \sim 600$ digits

$$X^E \pmod{N}$$