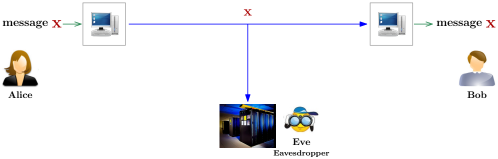
Number Theory & Cryptography

- Divisibility and Congruence
- Modular Arithmetic and its Applications
- GCD, (Extended) Euclidean Algorithm, Relative Prime
- The Caesar Cipher and Affine Cipher, Modular Inverse
- The Chinese Remainder Theorem
- Fermat's Little Theorem and Modular Exponentiation
- Private and Public Key Cryptography, The RSA Cryptosystem

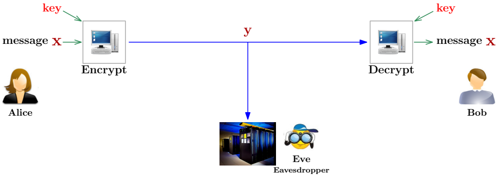
Imdad ullah Khan

Private Key Cryptography

Alice sends message to Bob, Eve eavesdrops



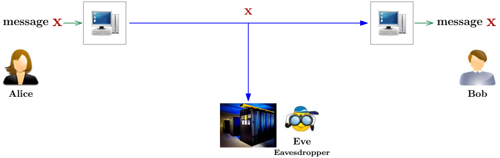
Exchange the encryption key for a good cipher!



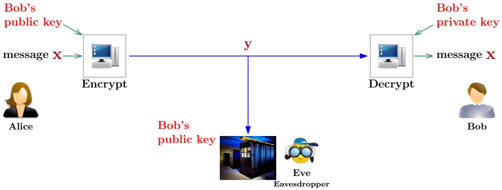
But during **key exchange**, Eve could get the key and all security is lost!

Public Key Cryptography

Alice sends message to Bob, Eve eavesdrops



Everyone knows public key, only Bob knows private key



Alice encrypts with public key, Bob decrypts with private key

Eve cannot do anything! ▷ No key exchange

Public Key Cryptography: RSA

Keys generation

- Choose two large primes p and q ▷ p and q are secret
- Set $n = pq$ and $T = (p-1)(q-1)$
- Choose e such that $\text{GCD}(e, T) = 1$ ▷ e^{-1} exists
- choose $d = e^{-1}$ modulo T ▷ $de \equiv_T 1$
- e and n are public keys ▷ published on Internet
- d is private key ▷ only Bob knows it

Public Key Cryptography: RSA

Encryption

- Encode message as an integer $M < n$
- Compute $C = M^e \% n$ ▷ Use modular exponentiation!

▷ Encryption does not require private key

Decryption

- Compute $M = C^d \% n$ ▷ Use modular exponentiation!

Public Key Cryptography: RSA

Keys generation

- Choose two large primes p and q
- Set $n = pq$ and $T = (p-1)(q-1)$
- Choose e such that $\text{GCD}(e, T) = 1$
- choose $d = e^{-1}$ modulo T
- e and n are public keys
- d is private key

Example Keys

- $p = 59$ and $q = 43$
- $n = 2537$ and $T = 2436$
- $e = 13$: $\text{GCD}(13, 2436) = 1$
- $d = 937 = 13^{-1}$ modulo T
- 13 and 2537 are public keys
- 937 is private key

Encrypt "STOP" $S \to 18, T \to 19, O \to 14, P \to 15 \implies 1819\ 1415$

$C = M^e \ \% \ n$ $\quad 1819^{13} \ \% \ 2537 = 2081 \quad 1415^{13} \ \% \ 2537 = 2182$

Encrypted message is 2081 2182

Public Key Cryptography: RSA

Keys generation

- Choose two large primes p and q
- Set $n = pq$ and $T = (p-1)(q-1)$
- Choose e such that $gcd(e, T) = 1$
- choose $d = e^{-1}$ modulo T
- e and n are public keys
- d is private key

Example Keys

- $p = 59$ and $q = 43$
- $n = 2537$ and $T = 2436$
- $e = 13$: $gcd(13, 2436) = 1$
- $d = 937 = 13^{-1}$ modulo T
- 13 and 2537 are public keys
- 937 is private key

Decrypt "0981 0461"

$M = C^d \ \% \ T \qquad 0981^{937} \ \% \ 2537 \ = \ 0704 \qquad 0461^{937} \ \% \ 2537 \ = \ 1115$

$07 \rightarrow H, 04 \rightarrow E, 11 \rightarrow L, 15 \rightarrow P \implies$ "HELP" ▷ message is "HELP"

RSA: Proof of Correctness

We need to show that

- $C^d \,\%\, n$ is indeed equal to M ▷ Correctness
- Without knowing d cannot compute M from C ▷ Security

RSA: Proof of Correctness

Theorem (Correctness of RSA)

$C^d \ = \ (M^e)^d \ \equiv_n \ M$

Proof: $de \equiv_T 1$ Thus, $\exists\, k \in \mathbb{Z} : de = 1 + k(p-1)(q-1)$. So

$$C^d \ = \ M^{de} \ \equiv_{pq} \ M^{1+k(p-1)(q-1)}$$

- $C^d \ = \ M(M^{p-1})^{k(q-1)} \ \equiv_p \ M \cdot 1^{k(q-1)} \ \equiv_p \ M$
- $C^d \ = \ M(M^{q-1})^{k(p-1)} \ \equiv_q \ M \cdot 1^{k(p-1)} \ \equiv_q \ M$ $\triangleright$ FLT

Hmm! a system of modular equations with $\text{GCD}(p, q) = 1$

$C^d \equiv_{pq} M$ is a solution to this system and by CRT its a unique solution

RSA: Proof of Security

Without knowing d cannot compute M from C ▷ Security

It is believed to be very hard to find p and q given $n = pq$

Prime factorization is a difficult problem

▷ though we do not have theoretical proof for it