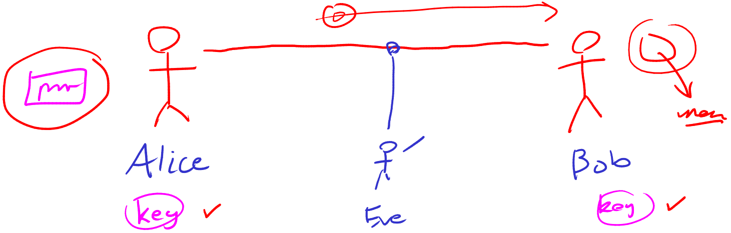
Public-key cryptography

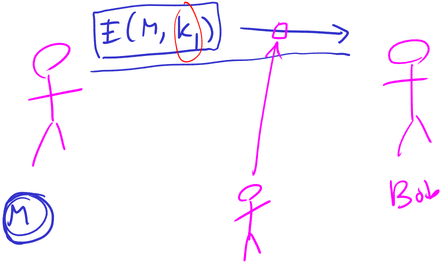


public key k_1

private key k_2

Bob: 121134

Private key cryptography



$D(E(M,k_1),k_2) \Rightarrow M$

$k_1 = 121134$

$\boxed{k_2}$

RSA

Rivest

Shamir

Adelman

Public key $\underline{(e, n)}$ big number

Private key (d, n)

<u>Message</u> : m

- $\text{encrypt}(m) = (m^e) \underline{\text{mod}}\ n$ %
- $\text{decrypt}(r) = (r^d) \text{ mod } n$

Pick two prime numbers : $\boxed{p, q}$

$\boxed{\underline{n} = pq}$

pick $\boxed{e}$ 65535

Calculate d : $\boxed{e^{-1} \ (\text{mod } (p-1)(q-1))}$

RSA

$$(m^e) \bmod n$$

$$(a+b) \bmod n$$

$$\parallel$$

$$((a \bmod n)+(b \bmod n)) \bmod n$$

$$(a \cdot b) \bmod n$$

$$\parallel$$

$$((a \bmod n)(b \bmod n)) \bmod n$$

RSA: steps

- Private key: (d, n), Public key: (e, n)
- Encryption $E(m) = m^e \bmod n$, Decryption: $D(w) = w^d \bmod n$.
- Goal: Select e, d, n such that $D(E(m)) = m^{ed} \bmod n = m$.