Public key cryptosystems

Alice → Bob

encrypt using Bob's public key

decrypt using his private key

DES / AES :

A ↔ B

key k key k

symmetric encryption

RSA

Bob chooses

- large random primes p, q (MUST BE RANDOM) $N = pq$
- chooses e (DOES NOT NEED TO BE RANDOM), computes d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$

$\phi(pq) = \phi(N)$

public key	private key
$N = pq$, e	d

Alice encrypts : $c \equiv m^e \pmod N$

Bob decrypts : $m \equiv c^d \pmod N$

$(m^e)^d = m^{ed} \equiv m$

EG

Bob's public key $(N = 33, e = 3)$

- encrypt $m = 4$ $\quad c \equiv m^e \pmod N$, $4^3 \pmod{33} = 31$
- determine private key d $\quad d = e^{-1} \pmod{\phi(N)}$, $3^{-1} \pmod{20} = 7$
- decrypt $c = 31$ $\quad m \equiv c^d \pmod N$, $31^7 \pmod{33} \equiv 4$

$\phi(33) = \phi(3)\phi(11) = 2 \cdot 10 = 20$