Encryption

- Encryption key k
- Encryption algorithm E_k
- Decryption algorithm D_k
- A given message: m
- a) $D_k(E_k(m))=m$
- b) D_k and E_k can be computed efficiently
- c) The security of the system depend only on the secrecy of the key and not on the secrecy of the algorithms

Encryption

- Public encryption key is a pair (e,n)
- Public decryption key is a pair (d,n)
- e, d, n are positive integers
- The functions E and D are defined as:
- $E(m) = m^e \bmod n = C$
- $D(C) = C^d \bmod n$
- n is computed as the product of two large randomly chosen prime numbers p and q

Encryption

-
- n = p x q
-
- Greatest Common Divisor [d, (p-1)x(q-1)] = 1
-
- e x d mod (p-1)(q-1) = 1

Encryption

- Example
- p=5, q=7 => n = 35
- (p-1)(q-1) = 24
- 11 is relatively prime to 24 => d = 11
- Since 11 x 11 mod 24 = 121 mod 24 = 1, e = 11
-
- Suppose m = 3
-
- $C = m^e \bmod n = 3^{11} \bmod 35 = 12$
- $C^d \bmod n = 12^{11} \bmod 35 = 3$