Public Key Crypto Using the RSA Algorithm

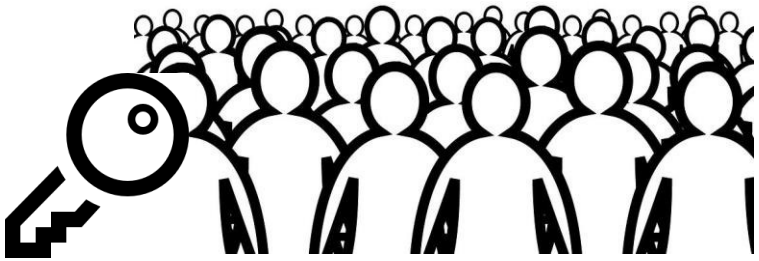
Dr Rosanne English

Asymmetric (Public Key)

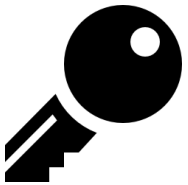
Uses a different key for encryption and decryption

Need to generate key pairs

- One is private, the other is public



Alice Public



Alice Private

RSA Key Generation

- Pick two large distinct random primes (p and q)
- Calculate n= pq
- Calculate $\phi(n) = (p-1)(q-1)$
- Pick e= number less than $\phi(n)$, co-prime to $\phi(n)$
- Calculate d
  - $d*e \equiv 1 \bmod \phi(n)$

- **Public** key is (e, n)
- **Private** key is (d,n)
- It is computationally infeasible to compute d from e and n alone

RSA Encryption and Decryption

Encryption

- Split message into blocks
- For each plaintext block B
  - $B^e \pmod{n}$

Decryption

- For each ciphertext block C
  - $C^d \pmod{n}$

public = (e, n)
private = (d,n)

RSA Toy Example- Key Generation

p q

$n = p \cdot q$

$\varphi(n) = (p-1)(q-1)$

$e < \varphi(n)$

e n

$d \equiv e^{-1} \bmod (\varphi(n))$

d n

$p = 5 \quad q = 11$

$n = 5 \cdot 11 = 55$

$\varphi(n) = 4 \cdot 10 = 40$

$e < 40$

$e = 7$

$d \equiv 7^{-1} \bmod 40$

$e \cdot d = 1$

$7d \equiv 1 \bmod 40$

$7 \cdot 23 \equiv 1 \bmod 40$

RSA Toy Example- Encryption

e, n

d, n

$P_1 P_2 \ldots$

$(P_1)^e \bmod n = C_1$

$(C_1)^d \bmod n \equiv P_1$

$e = 7 \quad d = 23$

$n = 55$

$B = 2$

$2^7 \bmod 55 = 128 \bmod 55$

$C_1 = 18$

$18^{23} \bmod 55 = 2$