

RSA Algorithm

Key Generation Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 9.5 The RSA Algorithm

Exercise :

$p=3, q=17, M=5, e=5$

$n = pq$ $= 3 * 17$ $= 51$	$\phi(n) = (p-1)(q-1) = 2 * 16 = 32$
Encryption by bob with Alice's public key : $C = M^e \pmod n$ $= 5^5 \pmod{51}$ $= 14$	$d \pmod{\phi(n)} = 1$ $d(5) \pmod{32} = 1$ $13(5) \pmod{32} = 1$ $d=13$
Encryption by bob with Alice's public key : $C = M^e \pmod n$ $= 5^5 \pmod{51}$ $= 14$	Decryption by Alice with Alice's private key : $M = C^d \pmod n$ $= 14^{13} \pmod{51}$ $= 5$

[RSA Cipher Calculator - Online Decoder, Encoder, Translator](#) - A link that can verify your d (private key) and C (cipher text)

Diffie-Hellman

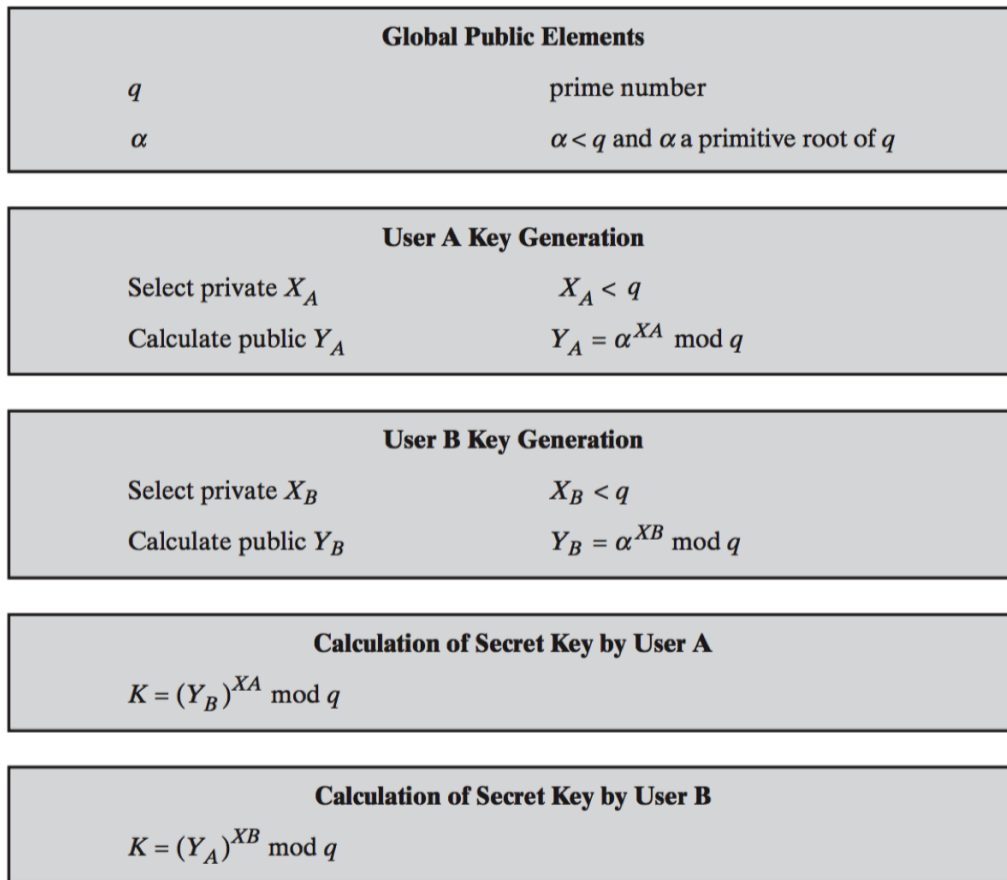


Figure 10.1 The Diffie-Hellman Key Exchange Algorithm

Exercise :

q = 23, α = 5, XA = 4, XB = 3		
A		B
YA = α ^ XA mod q YA = 5^4 mod 23 = 4 K = (YB)^XA mod q = 10^4 mod 23 = 18	Untrusted Network	YB = α ^ XB mod q YB = 5^3 mod 23 = 10 K = (YA)^XB mod q = 4^3 mod 23 = 18
∴ 18 is the secret key		

