# RSA Algorithm

| Key Generation Alice | |
|---|---|
| Select $p, q$ | $p$ and $q$ both prime, $p \neq q$ |
| Calculate $n = p \times q$ | |
| Calcuate $\phi(n) = (p-1)(q-1)$ | |
| 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: | $C = M^e \bmod n$ |

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

Figure 9.5 The RSA Algorithm

**Exercise :**

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

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

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

## Diffie-Hellman

| Global Public Elements | |
|---|---|
| $q$ | prime number |
| $\alpha$ | $\alpha < q$ and $\alpha$ a primitive root of $q$ |

| User A Key Generation | |
|---|---|
| Select private $X_A$ | $X_A < q$ |
| Calculate public $Y_A$ | $Y_A = \alpha^{XA} \bmod q$ |

| User B Key Generation | |
|---|---|
| Select private $X_B$ | $X_B < q$ |
| Calculate public $Y_B$ | $Y_B = \alpha^{XB} \bmod q$ |

| Calculation of Secret Key by User A |
|---|
| $K = (Y_B)^{XA} \bmod q$ |

| Calculation of Secret Key by User B |
|---|
| $K = (Y_A)^{XB} \bmod q$ |

**Figure 10.1** The Diffie-Hellman Key Exchange Algorithm

**Exercise :**

<table>
<tr><td colspan="3">q = 23, α = 5, XA = 4, XB = 3</td></tr>
<tr><td>A</td><td rowspan="2">Untrusted Network</td><td>B</td></tr>
<tr><td>YA = α ^ XA mod q<br>YA = 5^4 mod 23<br>= 4<br><br>K = (YB)^XA mod q<br>= 10^4 mod 23<br>= 18</td><td>YB = α ^ XB mod q<br>YB = 5^3 mod 23<br>= 10<br><br>K = (YA)^XB mod q<br>= 4^3 mod 23<br>= 18</td></tr>
<tr><td colspan="3">∴ 18 is the secret key</td></tr>
</table>