"RSA algorithm"

this algm is developed by Rivest, Shamir and Adleman of MIT library.

this algorithm is Asymmetric algm two keys are used for Enc and Dec (public key and Private key).

→ the procedure of this algm are.

step 1- Select 2 large Prime numbers P, q which are kept secret.

step 2- Calculate the product $n = p * q$

this product is public. (known to others), the select of prime numbers P, q should be in such away even they it's product value 'n' is known but their Prime factors (p, q) should not be known.

calculate the product

$\phi(n) = (p-1)(q-1)$ which is kept Secret.

Step 4: Select an integer 'e' (encryption key) such that is relative Prime to $\phi(n)$, i.e

$\gcd(e, \phi(n)) = 1$.

Step 5: Calculate an integer 'd' (decryption key) such that

'd' is a modular inverse of 'e' with modular value of $\phi(n)$.

→ it means $(e * d) \bmod \phi(n) = 1$ OR

$d = e^{-1} \bmod \phi(n)$.

{ such that this equation is true. }

→ public key = $\{e, n\}$.

→ private key = $\{d, n\}$.

ption

Consider the plain text is 'p' and the cipher text is 'c' is calculate by using public key (e,n) as:

المفتاح العام

$$c = p^e \bmod n$$

Decryption :- the plain text 'p' calculate as:

المفتاح الخاص

$$p = c^d \bmod n$$

ex:- consider $p=3$, $q=11$

Sol:-

* $n = p * q = 3 * 11 = 33$.
* $\phi(n) = (p-1)(q-1)$
  $= (3-1)(11-1) \Rightarrow 2 * 10 = 20$.

t an integer 'e' = 3

$$\gcd(e, \phi(n)) = 1$$

عددان أوليان يكون
محصور بين بحيث يكون
أكبر من الواحد والصفر فقط $\phi(n)$.
وكذلك يجب أن يكون العامل
المشترك الأكبر بينهما هو
$\phi(n) = 1$
أولي بالنسبة $\phi(n)$.

العامل المشترك الأكبر.

$$\gcd(3, 20) = 1$$

greatest common divisor.

- Calculate d where

$$(e * d) \bmod \phi(n) = 1$$

$$3 \times d \bmod 20 = 1$$

نفرض أعداد.
فحين الوصول إلى عدد
بحيث يكون ناتج القسمة 1

$d = 7$ ← لأن

$21 \bmod 20 = 1$

لأن $\frac{21}{20} = 1$ والباقي 1

- public key (3, 33)

- private key (7, 33)

محطة

* Encryption: Assume that $p = 5$ then

$$c = p^e \bmod n$$

$$= 5^3 \bmod 33 \Rightarrow 125 \bmod 33$$

$$= 26$$

*decryption: $p = c^d \bmod n$

$$= 26^7 \bmod 33 = 5 \leftarrow \text{p.t}$$

(c.t)