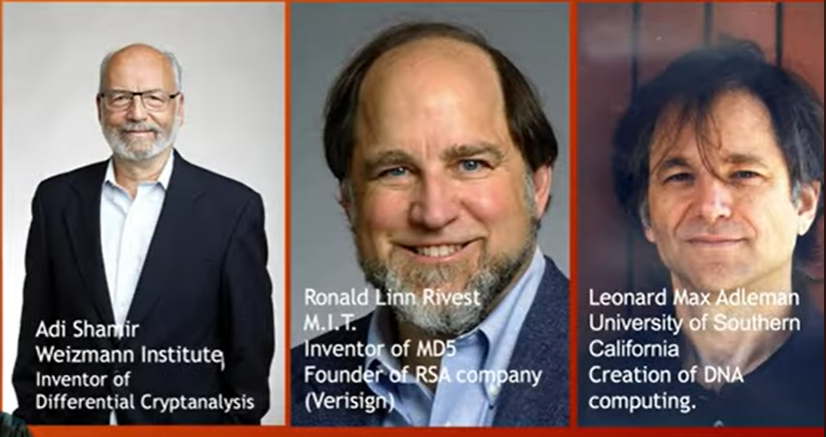
RSA Algorithm for Cryptography:

RSA Inventor:



* The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.
* The **RSA (Rivest-Shamir-Adleman) algorithm** uses two different keys: one for encryption and another for decryption.

How to does it work?

* How to make a public key:
* Choose two very large prime numbers, p and q.
* Let N = p \* q
* Let T = (p-1)(q-1) This is called the Euler Totient
* Choose two numbers “e” (stands for encryption) and “d” (stands for decryption) where (e\*d) mod T = 1
* Publish n and e. This is your public key.
* Keep n and d secret. This is your private key.

1, Key generation

* Choose two large prime numbers (p) and (q).
* Calculate their product (n = p\*q). And the value of (n) is part of the public key.
* Calculate the Euler’s totient function of (n), φ(n) or T = (p-1) \* (q-1).
* Choose an integer (e), such that 1 < e < T and [gcd(e, T)=1]. The value of (e) is part of a public key.
* Calculate the modular multiplicative inverse of (e) modulo T, which anther integer (d). The value of d is a private key.

2, Public Key: (n, e)

* n: The modulus, which is the product of the two large prime numbers.
* e: The public exponent, used for encryption.

3, Private Key: (n, d)

* n: The modulus, The same as in the public key.
* d: The private exponent, used for decryption.

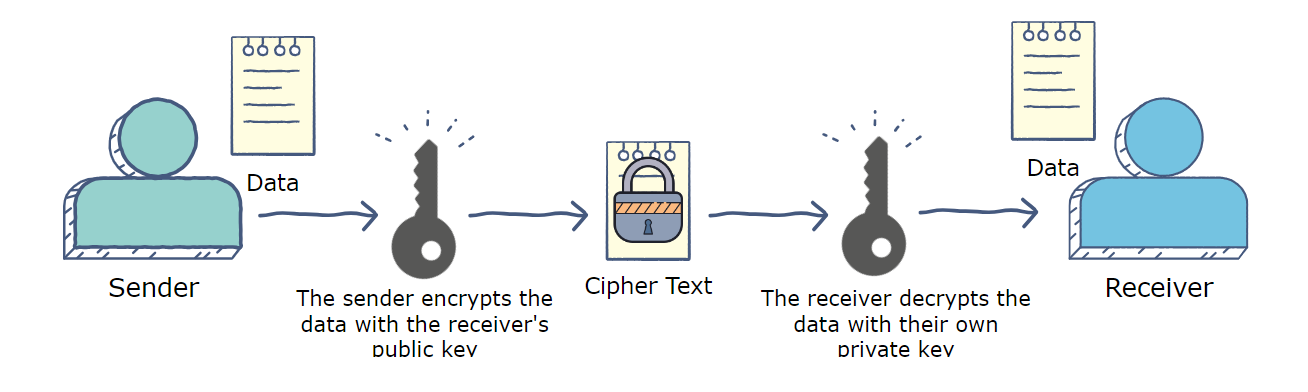
4, Encryption:

* To encrypt a message (M) represented as an integer into a cipher text: (C)

C = (mod n)

5, Decryption:

* To decrypt the cipher-text (C) back to the original message (M)

M = (mod n)

* For example:
* Key generation:
* Choose two prime numbers (p)= 2 and (q)=7
* Calculate (n: p\*q) = 2 \*7 = 14
* Calculate T = (p-1) \* (q-1) = 1\*6= 6
* Choose {(e, d) mod 6 =1} [e: encryption, d: decryption]; [Note: e and T should be relatively prime, and d is the inverse of e in mod T]
* Choose e =5, d=11

So, the public key is (14, 5) And The private key is (14, 11)

* How to encrypt a message:
* The published key is (14, 5)

So, let’s send a one-letter secret message “B”, Instead of (B) Let’s use the number 2.

Suppose: A=1, B=2, C=3 and etc.

We get Encryption value = mod 14 is 4.

Therefore, the encrypted value is 4. The encrypted message of 4 will be translated to letter ‘D’ if we were to translate directly.

* How to decrypt a message:
* The private key is (14, 11)

So, we know that the secret value is 4

Supposed: A=1, B=2, C=3…. Etc.

We get the decrypted value = mod 14

= 4,194,304 mod 14

4,194,304/14 We get remainder 2

Therefore: 2 is a decrypted message which is letter “B”