Intro To RSA

RSA is the oldest two key Asymmetric cryptography systems.

Each participant has two keys. One private and one public.

One participant uses a key to encrypt a message and the other uses a key to decrypt it.

The key used to encrypt messages are public and the key used to decrypt messages are private.

One participant can encrypt messages using the others public key that only the other can decrypt with their private key.

The advantage is that the participants don't have to exchange keys ahead of time, which is useful in long distances.

The disadvantage is the it is slow.

RSA provides a secure way for any two people to communicate over a secure channel.

History

The idea of asymmetric cryptography was created by Whitfield Diffie & Martin Hellman.

The idea was to make usage of a easy one-way function that was hard to compute in reverse.

Rivest and Shamir proposed one-way function ideas while Adleman found weaknesses.

Basic Concept

Two different keys; One for encryption and the other for decryption.

Public(known by everyone) and private key(known and used by the owner; kept secret).

Encryption and Decryption

Sender uses public key of the intended receiver to encrypt a message.

Only the owner of the according private key is able to decrypt the message.

Signature

Creator of the message encrypts a fingerprint(signature) of the message using his private key

To check the signature, everyone may use the public key of the creator.

Modular arithmetic

45 % 27 = 18

One way function

prime factorization finding the multiples of two prime numbers.

RSA

1. Chose two big prime numbers: p & q (must be 1024bit or more.)

1. Multiply these numbers to get: n

1. Calculate Euler's totient function (n) = (p-1) x (q-1)

1. Choose a number which shares no divisor with (n)

This means, that gcd(e (n)) = 1

Every prime number < (n) can be used

1. Calculate numbers k and d using the extended Euclidean algorithm

e d + k (n) = 1 or e d = k (n) + 1

it follows, that: e d mod (n) = 1

Public key is (e, n) and private key is (d, n)

Important

Delete p,q because they can be used to compute d & e

Encryption/ Decryption

Sender converts text into a number(m) from the ASCII smaller than n

Sender calculates c = m^e mod n (using receiver's public key)

Receiver calculates m = c^d mod n (using receiver's private key)

Receiver converts number m into text.

a & b are relatively prime (or coprime) if GCD(a, b) =1

RSA (Example)

1. p = 13 q = 23
2. n = 299 = 13 x 23
3. (n) = (13-1) x (23-1)

=12 x 22 = 264

1. e = 17
2. Use the Euclidean algorithm to find d,-k in e d + k (n)= 1

k = 15 d= 233

Thus

Public key : (17, 299)

Private key: (233, 299)

Hybrid Crypto System uses Asymmetric cryptograph to exchange keys and symmetric

to encrypt messages.