Cryptography

Hieroglyph

The first known evidence of cryptography can be traced to the use of ‘hieroglyph’. Some 4000 years ago, the Egyptians used to communicate

History of Cryptography

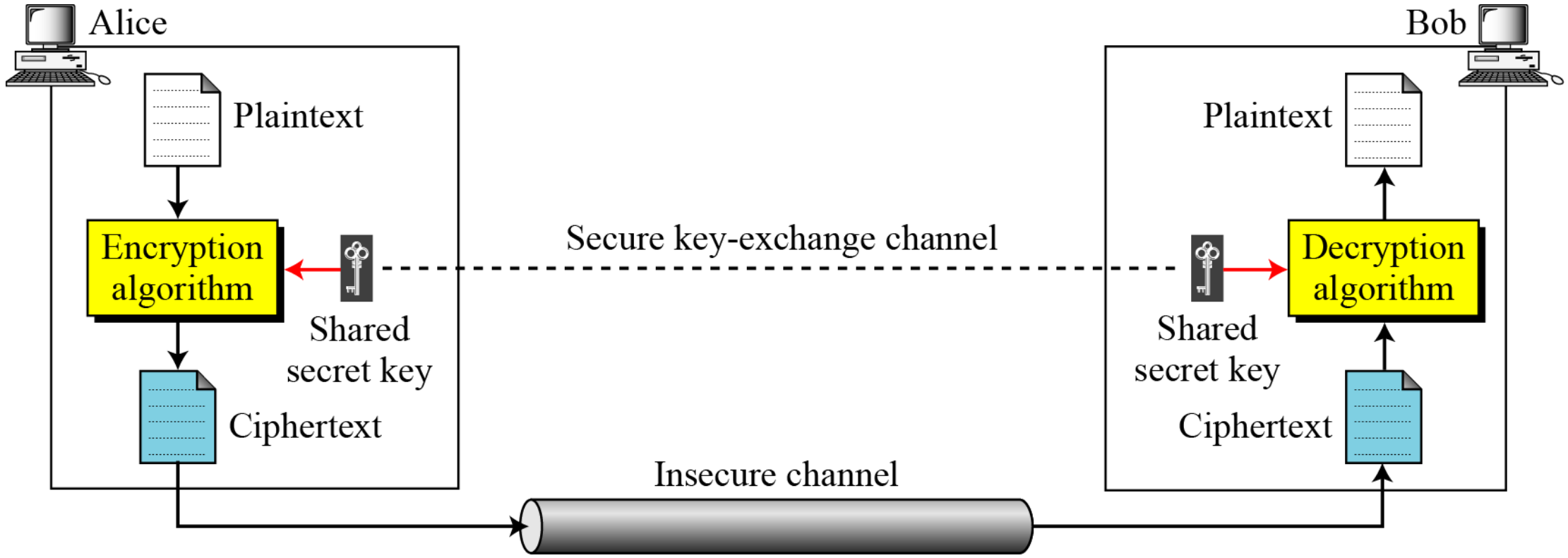
Cryptography (Basic definition)

- It is the science and art of transforming messages to make them secure and immune to attacks.

Different types of Cryptography

- Symmetric Key Cryptography : Same key will be used for encryption & decryption.
- Asymmetric Key Cryptography: One key will be used for encryption and another key will be used for decryption.

Symmetric Key Cryptography



The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

- A few well-known examples of symmetric key encryption methods are

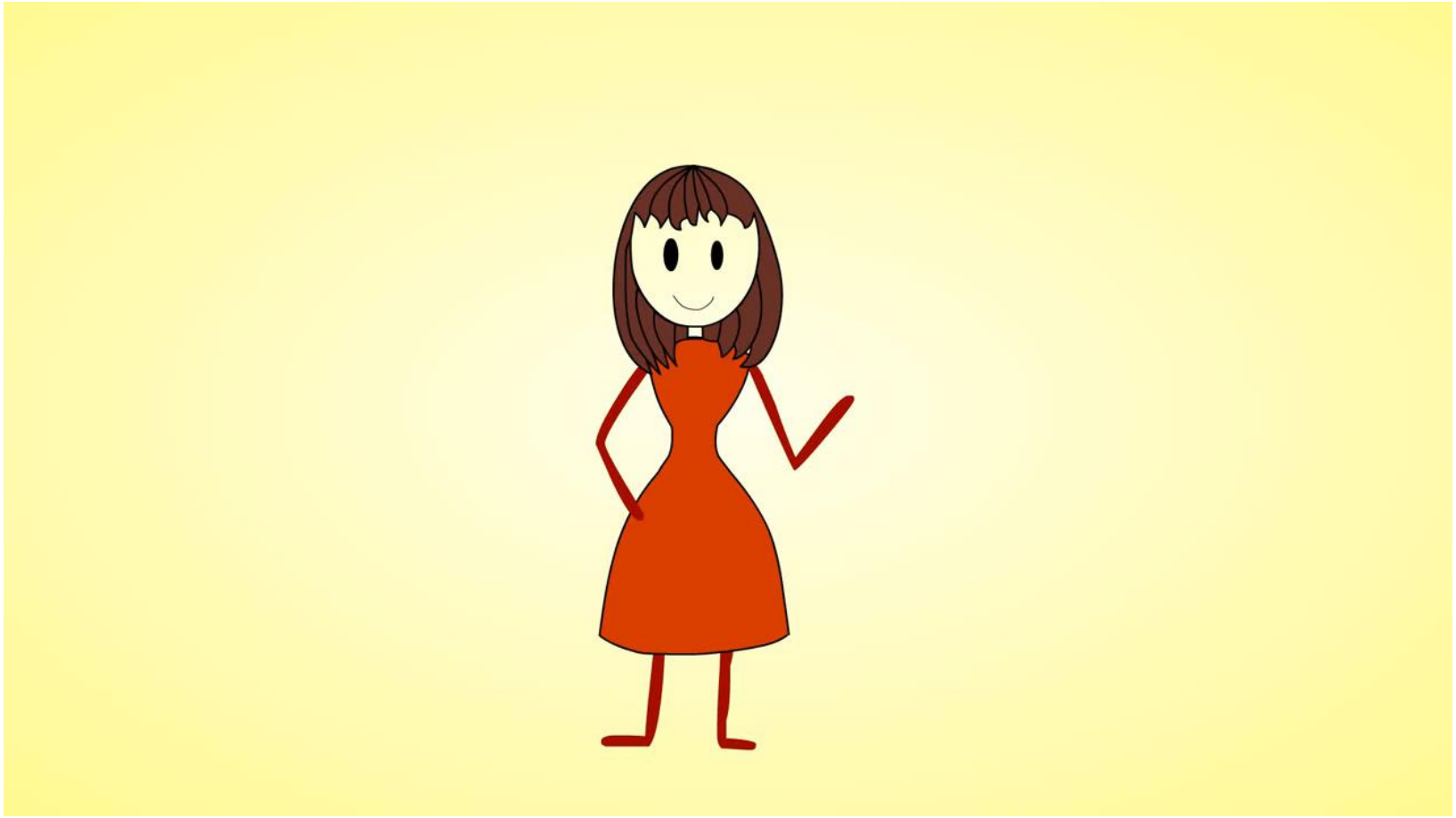
- Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

Challenge of Symmetric Key Cryptosystem

- **Key establishment** : Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.

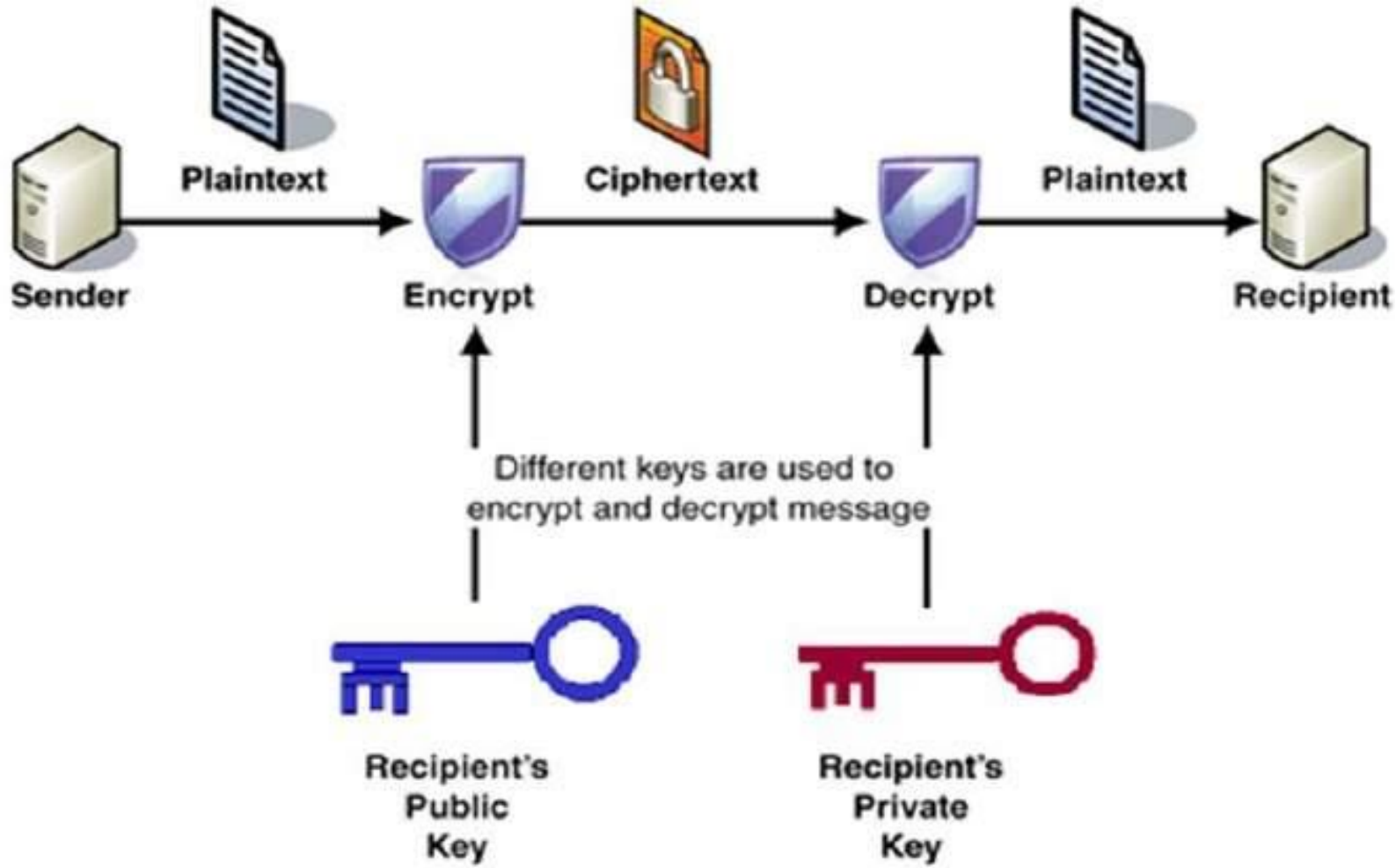
- **Trust Issue :** Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other.

Asymmetric Key Encryption



Asymmetric Key Encryption

- The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption.


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to
encrypt and decrypt message
Recipient's
Public
Key
Recipient's
Private
Key

Steganography

Not only protect the secrecy of an information by concealing it, but also to make sure any unauthorized person gets no evidence that the information even exists.

Security Attacks

- Passive attacks:
  - Attacker’s goal is to just obtain the information.
  - Attack dose not modify the data or harm the system.
  - Snooping: Unauthorized access to or interception of data.
  - Traffic analysis: Attempts of analyzing encrypted messages to come up with likely patterns.

Security Attacks

- Active attacks:
  - Attack may change the data or harm the system.
  - Modification: The attacker modifies the information.
  - Masquerading or Spoofing: It happens when the attacker is posing the identity of somebody else.

- Suppose that everyone in a group of N people wants to communicate secretly with the N–1 others using symmetric key cryptographic system . The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is

RSA

- RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

RSA

❖Choose two different large prime number p and q

Calculate n= p*q

Calculate ø(n)=(p-1)*(q-1)

Choose e such that 1<e<ø(n)

e Should be coprime to ø(n) i e. *e Gcd(e, ø(n))=1*

❖*Ex if* ø(n) is 20 then e should not be 5 or 2

❖Calculate d such that

$d.\ e \equiv 1 \bmod \phi(n)$ or

$d = (1 + k\,\phi(n))/e$

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

❖Public key e private key d

- P=3,q=11
- n=pxq=3x11=33
- ø(n)=(p-1)x(q-1)2x10=20
- Choose e such that e should be co prime
- Means it should not multiply by the factor of ø
- Factor of ø are =5x2x2, e should not be 5,2 and should not divide by 20
- e=7
- d=3

- In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____.
- **Note:** This questions appeared as Numerical Answer Type.
  (A) 11
  (B) 13
  (C) 16
  (D) 17

- Answer 11

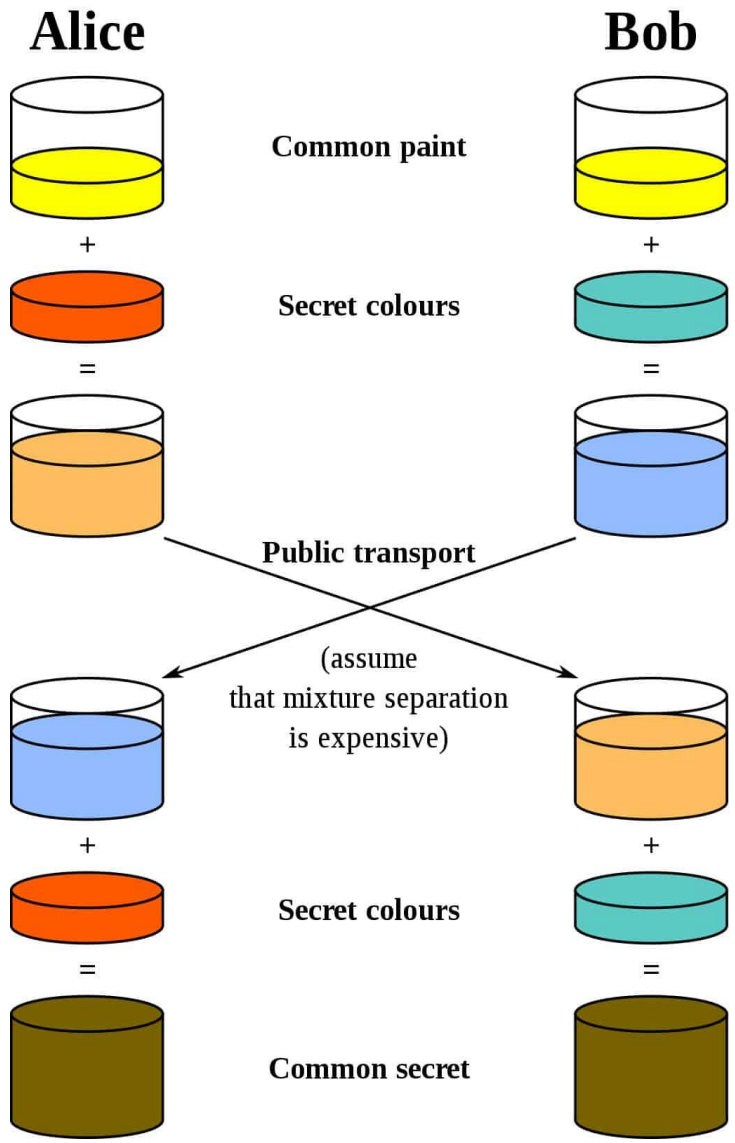
Diffie Hellman Key Exchange

- The main purpose of the Diffie-Hellman key exchange is to securely develop shared secrets that can be used to derive keys.

- The Diffie-Hellman key exchange is frequently implemented in security protocols such as TLS, IPsec, SSH, PGP, and many others.

- As part of these protocols, the Diffie-Hellman key exchange is often used to help secure your connection to a website, to remotely access another computer, and for sending encrypted emails

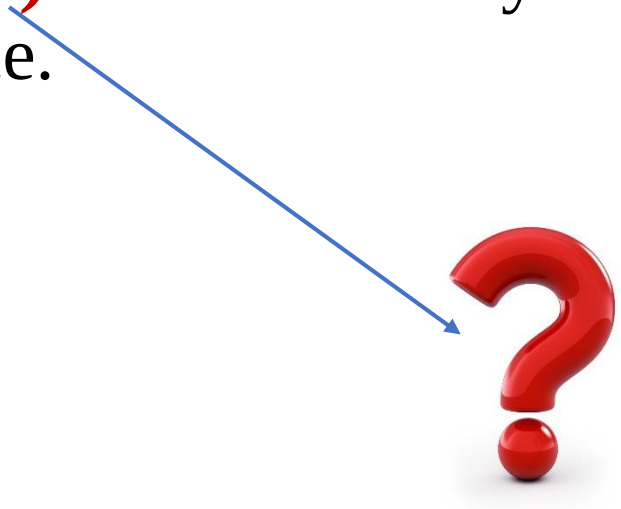
How does the Diffie-Hellman key exchange work?



- These are the modulus (p) and the base (g).

- In practical use, the modulus (p) is a very large prime number,
- while the base (g) is relatively small to simplify calculations.

- The base (g) is derived from a ***cyclic group (G)*** that is normally generated well before the other steps take place.



- (0,1,2,3,4) +4

- For our example, let's say that the modulus (p) is **17**, while the base (g) is **4**.

- Once they have mutually decided on these numbers, Alice settles on a secret number (**a**) for herself, while Bob chooses his own secret number (***b***). Let's say that they choose:
- $\boldsymbol{a = 3}$
- $\boldsymbol{b = 6}$

- Alice then performs the following calculation to give her the number that she will send to Bob:

  - $A = g^a \bmod p$

- So let's put our numbers into the formula:
- $A = 4^3 \bmod 17$
- $A = 64 \bmod 17$
- $A = 13$

- When we do the same for Bob, we get:
- $B = 4^6 \bmod 17$
- $B = 4096 \bmod 17$
- $B = 16$

- Alice then sends her result (A) to Bob, while Bob sends his figure (B) to Alice. Alice then calculates the shared secret (s) using the number she received from Bob (B) and her secret number (a), using the following formula:

- $s = B^a \bmod p$
- $s = 16^3 \bmod 17$
- $s = 4{,}096 \bmod 17$
- $s = 16$

- Bob then performs what is essentially the same calculation, but with the number that Alice sent him (A), as well as his own secret number (b):

- $s = A^b \bmod p$
- $s = 13^6 \bmod 17$
- $s = 4{,}826{,}809 \bmod 17$
- $s = 16$

Why is the Diffie-Hellman key exchange secure?

- On a mathematical level,
- These are calculations which are simple to do one way, but much more difficult to calculate in reverse.
- it is infeasible to calculate *gab* from the separate values of *g*, *ga* and *gb*. There is currently no publicly known way to easily find *gab* from the other values,

- Question
- Suppose that two parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is

- Primitive root = g = 3
  Modulus = p = 7
  Xa = 2 and Xb = 5

  $Ya = 3^2 \bmod 7 = 2$
  $Yb = 3^5 \bmod 7 = 5$

  We assume D-H key to be K.

  $K = Ya^{Xb} \bmod 7$
  $K = 2^5 \bmod 7 = 4$
  Or
  $K = Yb^{Xa} \bmod 7$
  $K = 5^2 \bmod 7 = 4$

Digital Signature