**TOPIC: SSL/TLS**

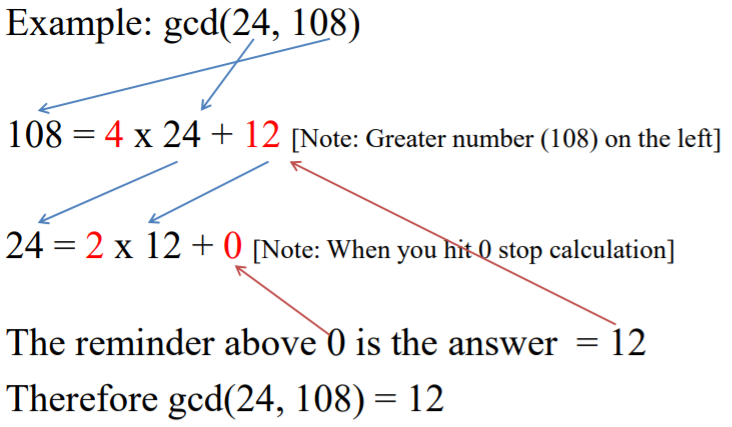
* WEAKNESS:

1. NO encryption to protect data; can be easily sniffed and read by anyone

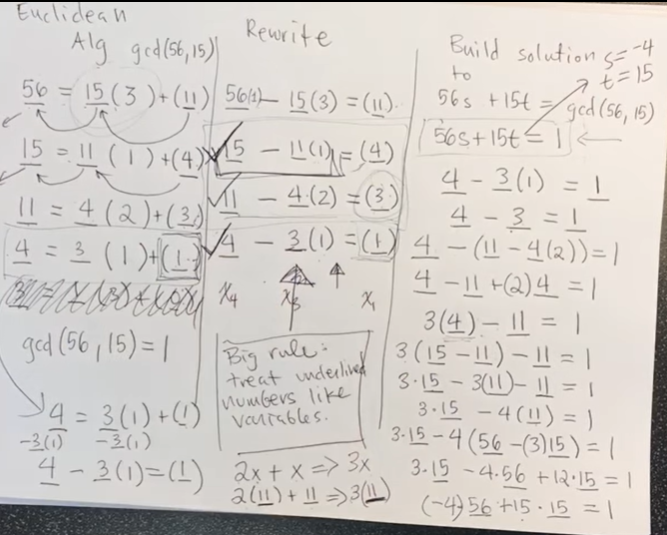
* TLS V1.2 AND TLS C1.3 ARE RECOMMENED FOR SECURITY
* PURPOSE OF TLS
  1. HANDSHAKE PROTOCOL
     + Establish shared secret key using public-key cryptography
     + Signed certificates for authentication
  2. RECORD LAYER
     + Transmit data using negotiated key, encryption function
* HANDSHAKE PROTOCOL
  1. Client Hello
     + Make a request to server by sending a random number and a set of Cipher Suite
  2. Server Hello
     + Server responds with
       - Random number
       - Chosen cipher
       - Server certificate
         * With server public key
  3. Client generation of pre\_master\_key and master\_key
     + Generation of pre\_master\_key
       - Verify server’s certificate and server’s CA certificate
       - Generate “pre\_master\_key”
       - Encrypt “pre\_master\_key” with server public key
       - Send the encrypted “pre\_master\_key” to server
     + Generation of master\_key
       - 3 number needed:
         * Client random number
         * Server random number
         * Pre\_master\_key
       - The 3 number will be use in a Key Derivation Function to compute the “master\_key”
     + Client change cipher spec
       - Inform server all message sent will be encrypted using master\_key
     + Client encrypted handshake message
       - Hashes all previously exchanged messages
       - Encrypt the message digest (MAC) with the master key using the agreed algorithm
       - Send the encrypted MAC code
  4. Server generation of master key
     + Decrypt the encrypted “Pre\_master\_key” using its private key
     + Generation of master\_key
       - 3 number needed:
         * Client random number
         * Server random number
         * Pre\_master\_key
       - The 3 number will be use in a Key Derivation Function to compute the “master\_key”
     + Decrypts the client’s encrypted handshake (MAC)
       - Using the Master\_key
       - Hashes all the previously exchanged messages
       - Compare the hash with decrypted MAC (to check it match or not)
         * To check if all the previously exchanged message were not tempered
         * If not match, server cancel the handshake with an alert protocol
     + Server change cipher spec
       - Inform client all message sent will be encrypted using master\_key
     + Server encrypted Handshake Message
       - Hashes all previously exchanged messages
       - Encrypt the message digest (MAC) with the master key using the agreed algorithm
       - Send the encrypted MAC code
  5. Verification of Server encrypted handshake message
     + Decrypts the server’s encrypted handshake (MAC)
       - Using the Master\_key
       - Hashes all the previously exchanged messages
       - Compare the hash with decrypted MAC (to check it match or not)
         * To check if all the previously exchanged message were not tempered
         * If not match, server cancel the handshake with an alert protocol
  6. Client and server will start encrypting the application data using the master key than send out. The other side will decrypt the encrypted data using the master\_key. This goes on until the client request termination

**TOPIC: NUMBER THEORY**

* Euclidean method



* Extended Euclidean

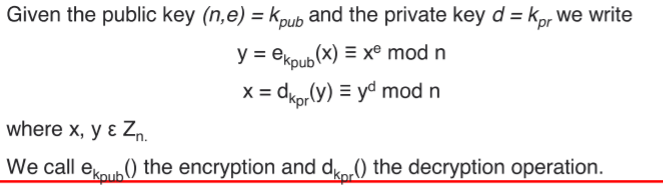


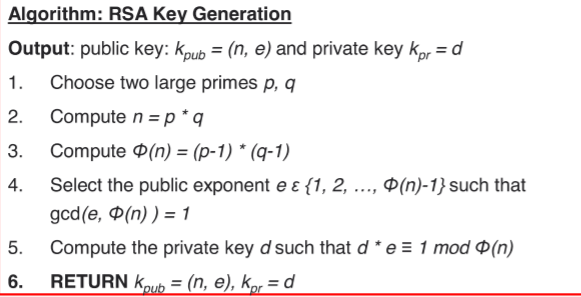
Ans: 15

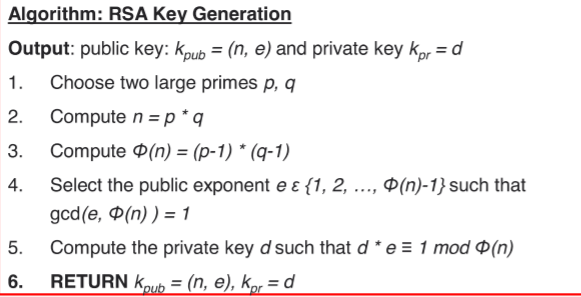
<https://www.youtube.com/watch?v=6KmhCKxFWOs>

**TOPIC: RSA**

* Mainly used
  + Transport of (i.e., symmetric) keys
  + Digital signatures
* Encryption and Decryption





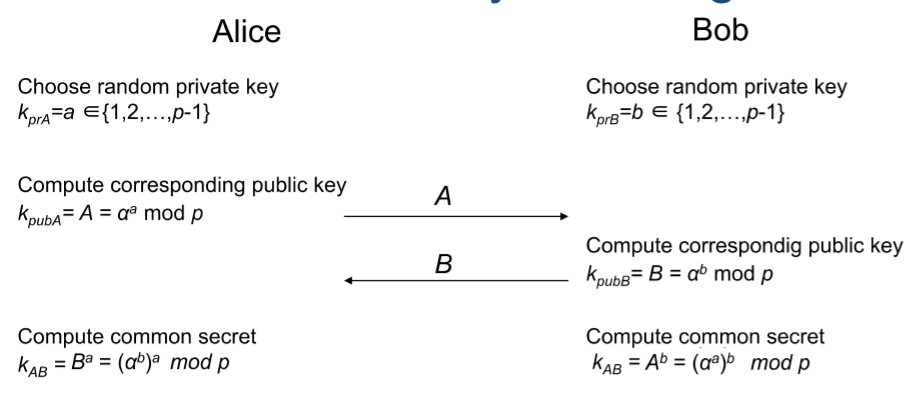


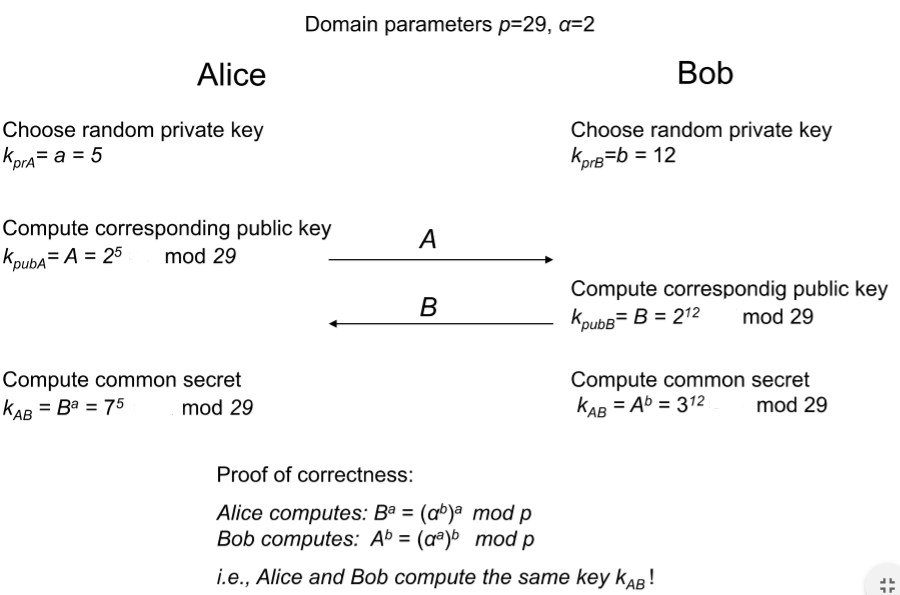
**(use Extended Euclidean)**

**4. d=**

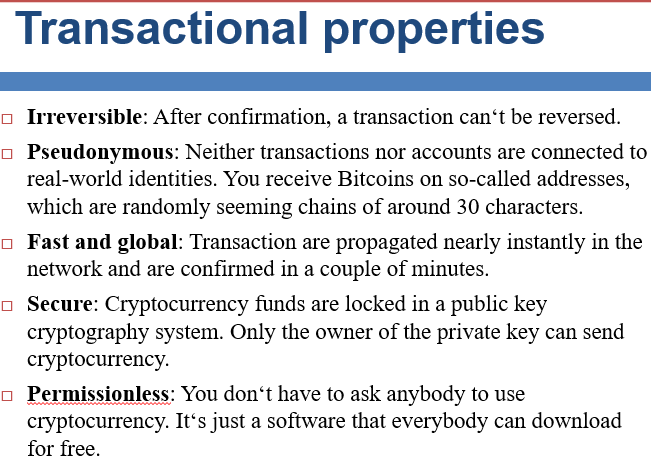
**TOPIC: DHE**

* Commonly used:
  + SSH
  + TLS
  + IPSec
* a key exchange protocol and not used for encryption
* To agree on a key that can be used for encryption, in a way that an eavesdropper cannot obtain the key
* “A” = public key
* “a” = private key



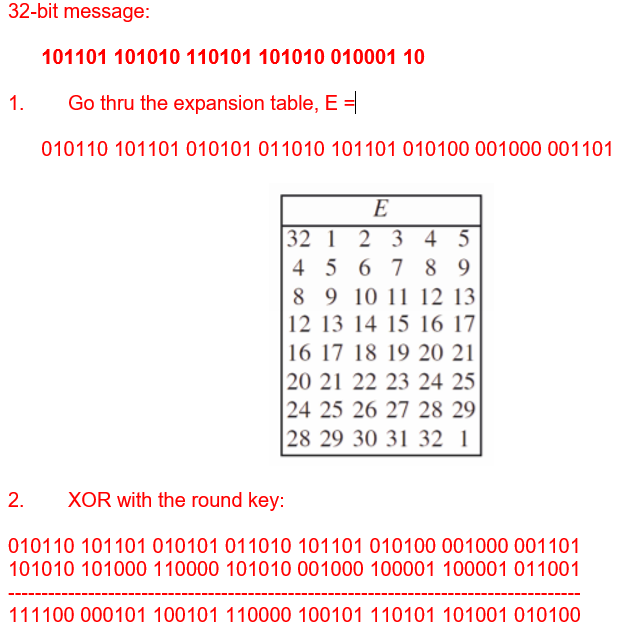


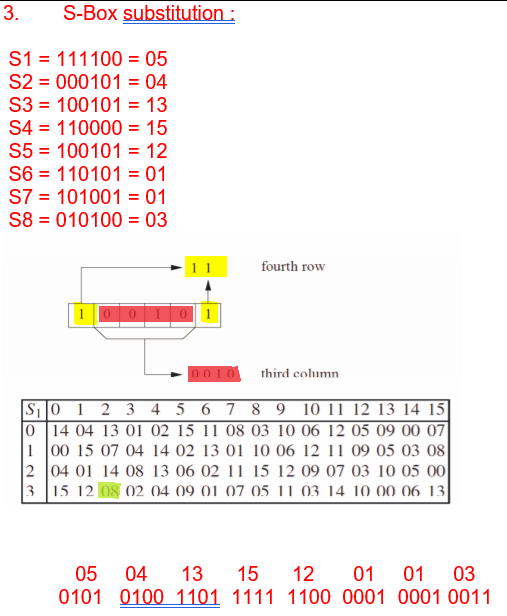
**TOPIC: CRYPTOCURRENCY**

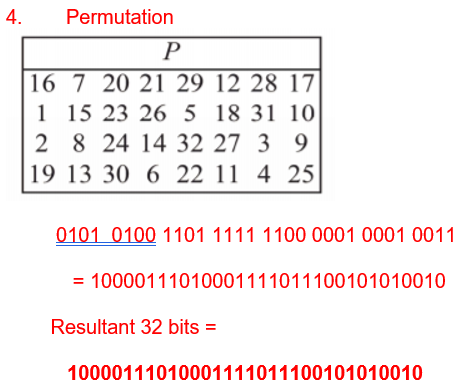


**TOPIC: DES**

* A type of block cipher
* Block Cipher Primitives operations
  + Use to build “Product ciphers”
  + CONFUSION:
    - An encryption operation where the relationship between key and ciphertext is obscured.
  + DIFFUSION:
    - An encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext.
      * simple diffusion element is the bit permutation
* Initial and Final Permutation
  + WIP
* F-Function







STUDY SECURITY OF DES

3DES NO NEED TO STUDY

TOPIC: AES

HIGH LEVEL DESCRIPTION OF THE AES ALGORITHM

AES OVERVIEW NEED TO STUDY

KEY ADDTION

BYTE

ROW

COLUMM

KEY ADDITION

KEY ADDITION LAYER COLUMM ORDER

BYTE SUBSTITUTION LAYER

SHIFTROW SUBLAYER

CBC: In CBC mode, each block of plaintext is XORed

with the previous ciphertext block before being

encrypted.