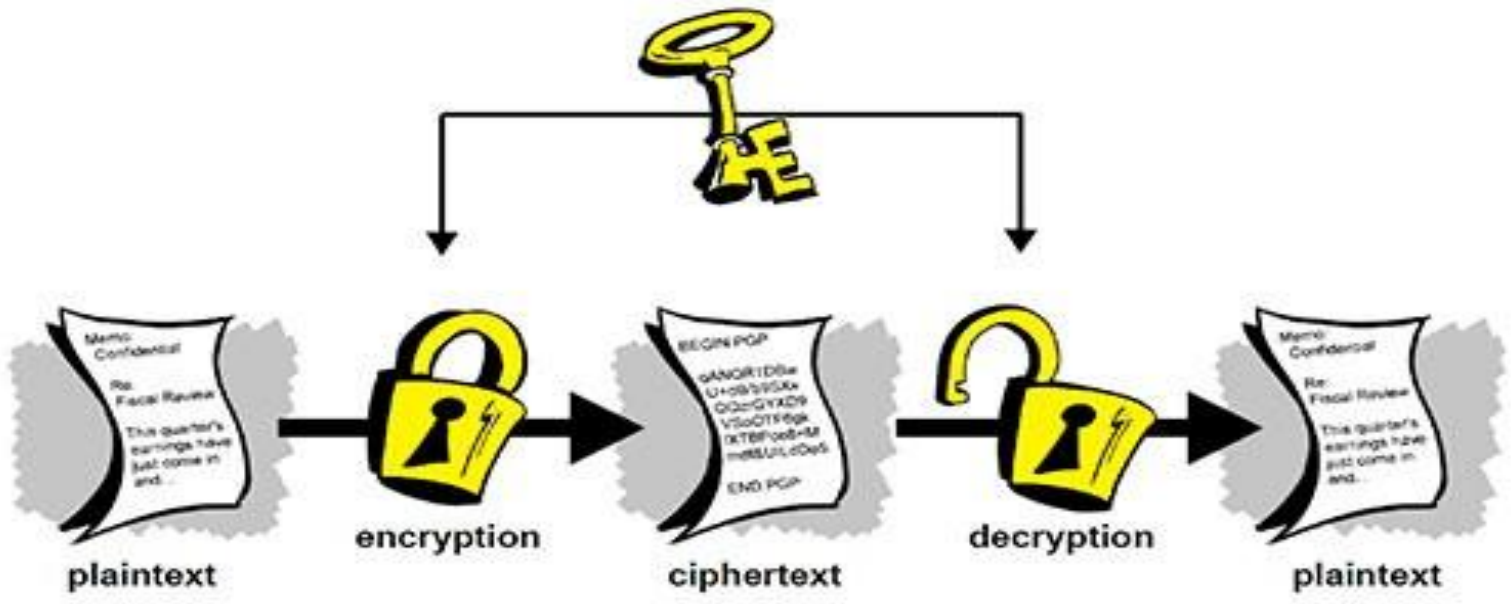
CT 1406

NETWORK SECURITY LAB

Lab 2&3. AES & RSA Encryption

The process of converting information or data into codes to prevent unauthorized access'



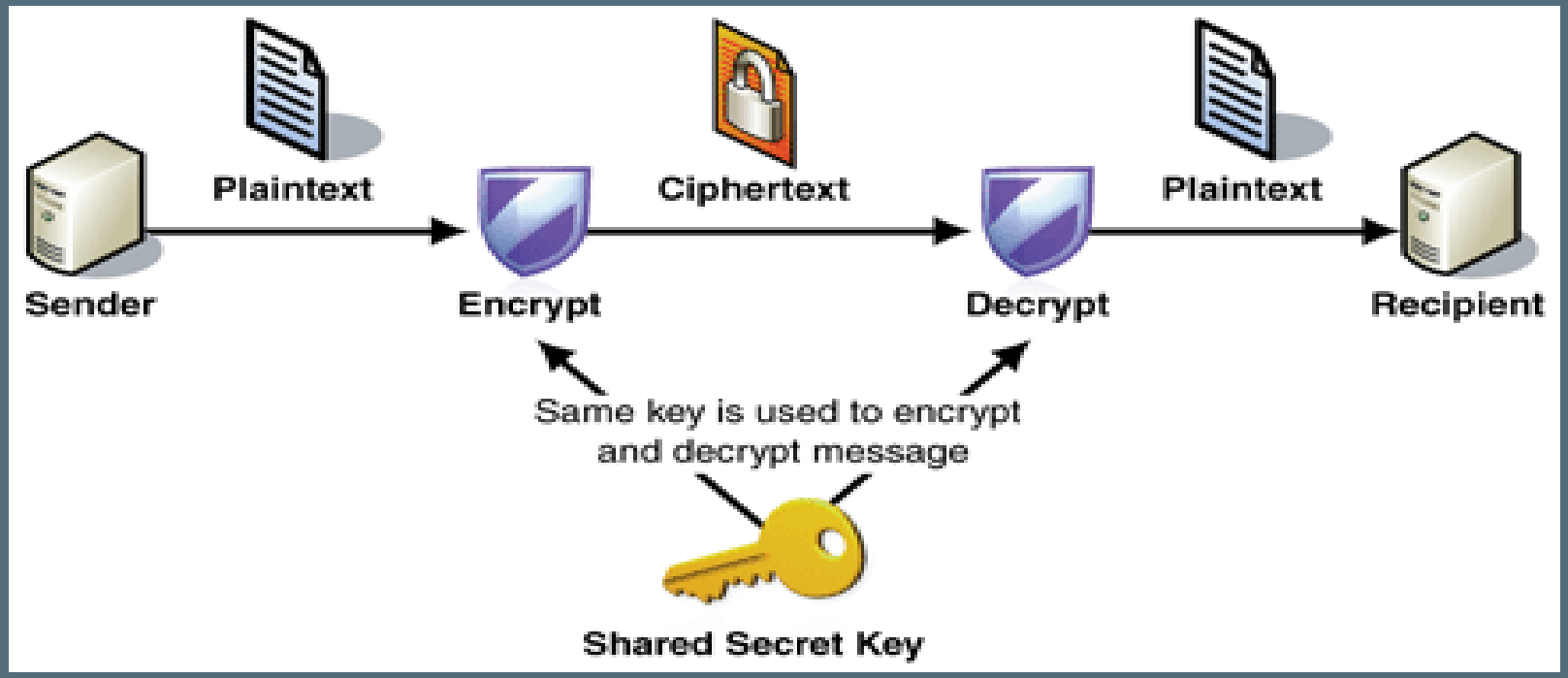
- *Data/Information – i*
- *Encrypted data = cipher = C*
- *Encryption Algorithm = E*
- *Encryption Key = K*
- *Decrypted data = plaintext = d*

$$i=E(K,C) \quad OR \quad C= E_K(i)$$

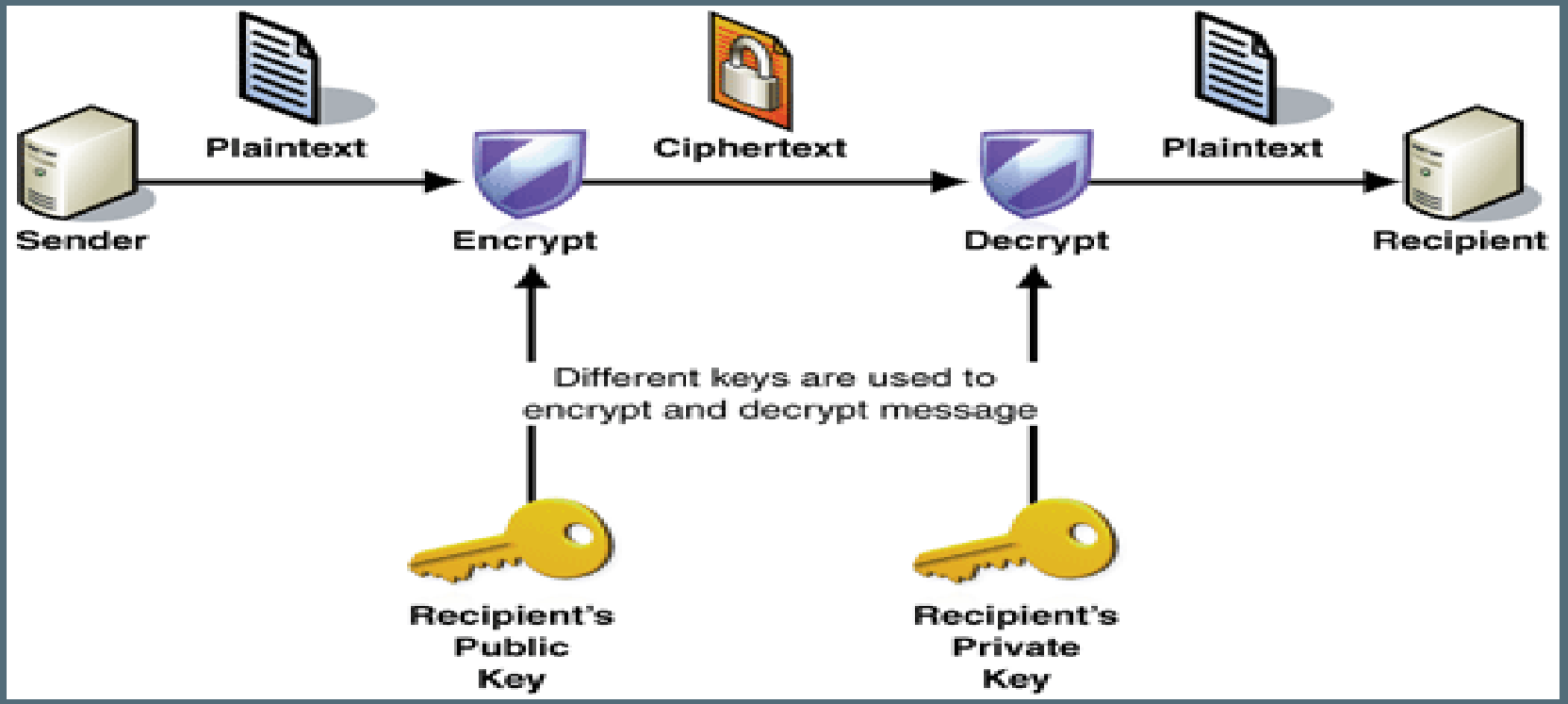
$$d=E(K,C) \quad OR \quad d=E_K(C)$$

- Encryption or Enciphering: Process of converting plain text to cipher text.
- Encryption Algorithm: Performs encryption
  - Inputs needed: plain text and secret key
- Deciphering or Decryption: Process of recovering plain text from cipher
- Secret Key: used for encryption or decryption

- *Symmetric Encryption: Process encryption where same key is used to encrypt and decrypt the data:*



- Asymmetric Encryption AKA PKI: Process encryption where public and private keys are used to encrypt and decrypt the data:

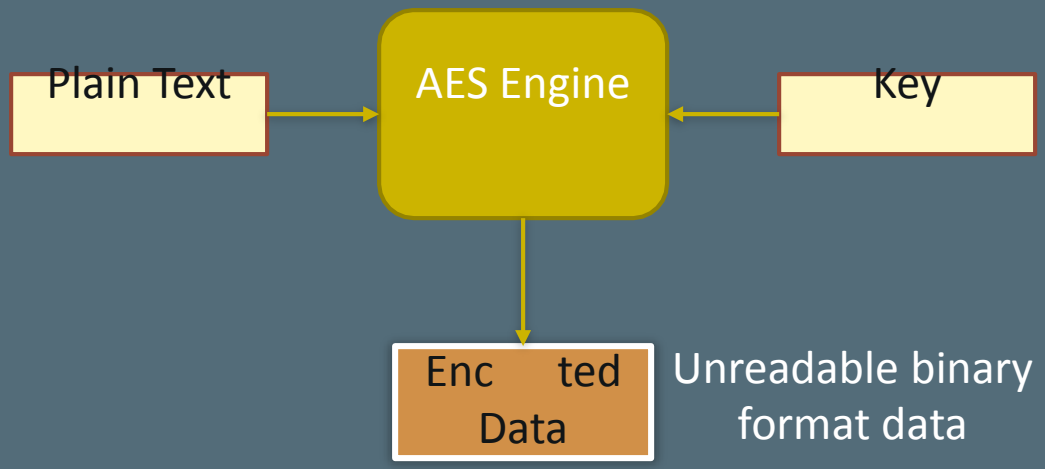


- Commonly used in database as there are no two separate end points to send and receive data.
- Widely used due to its speed factor compared to PKI.
- Often used in encrypting backup tapes for offline storage and digital streaming.
- Used to securely store private information, credit card information, etc.,

- Symmetric encryption uses a number of algorithms:
  - Two Fish (Open source)
  - Blow Fish
  - 3DES
  - DES
  - AES
- In late 1990's the National Institute for Standards and Technology (NIST) felt the need for new standard for cryptography.

- Belgian Cryptographers : Vincent Rijmen and Joan Daemen developed the AES.
- Acquired by Federal Government and named as FIPS197.
- Widely accepted by the private sector.
- Testing protocols for AES

- Requirements:
  - Software that implements the AES Algorithm
  - Inputs: Data (credit card number, plain text) and Key (encryption key)



Reversal for decryption

- AES is a block cipher
- Has an Initialization Vector (IV) for rounds of encryption for the data in the block.
- Size of the block is 16 bytes
- Encryption Key Sizes:
  - 128 bit (16 Bytes)
  - 192 bit (24 Bytes)
  - 256 bit (32 Bytes)

- Encryption Key – A passphrase
- Should be complex and not a easy guess
- Use combination of letters, numbers, cases and special characters.

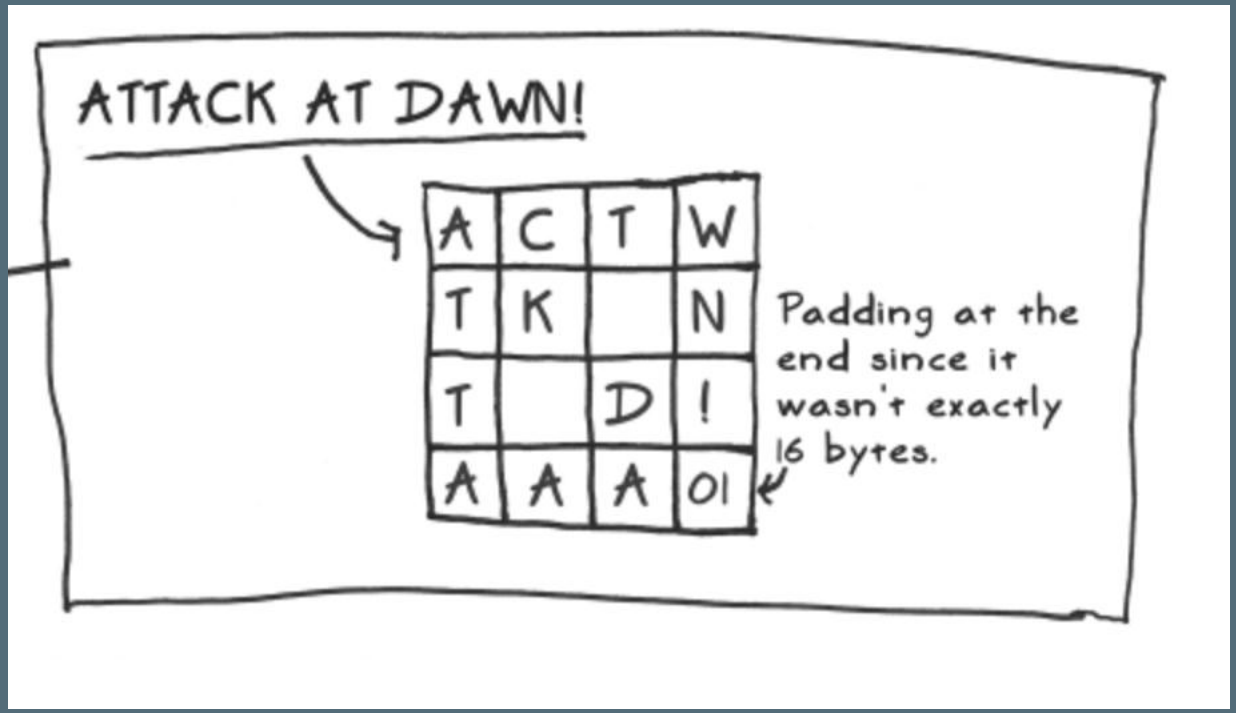
  Ex: PlayerR@g3!$$

- How keys are generated?
  - Random Number Generated (RNG)
  - Password Based Encryption (PBE) = Password + Software for encryption and hashing.
  - Split Passwords = Passwords entered by 2 or more users.

- Software Vendors:
  - Microsoft
  - IBM
  - SUN
- Products with Encryption
  - Third party vendors

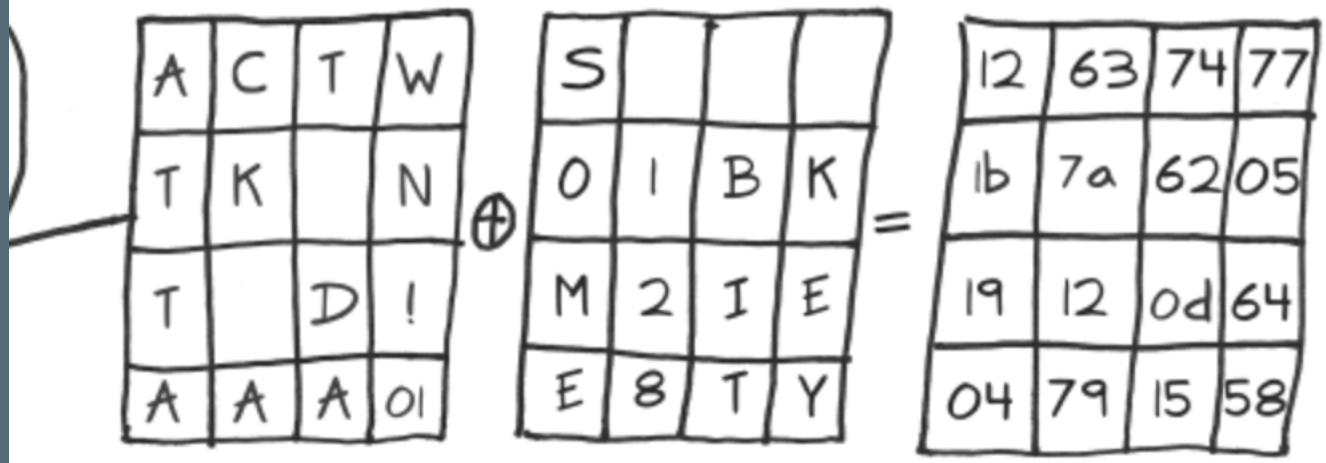
- Free subscriptions
  - Online applications
  - Free web applications

The plain text Message

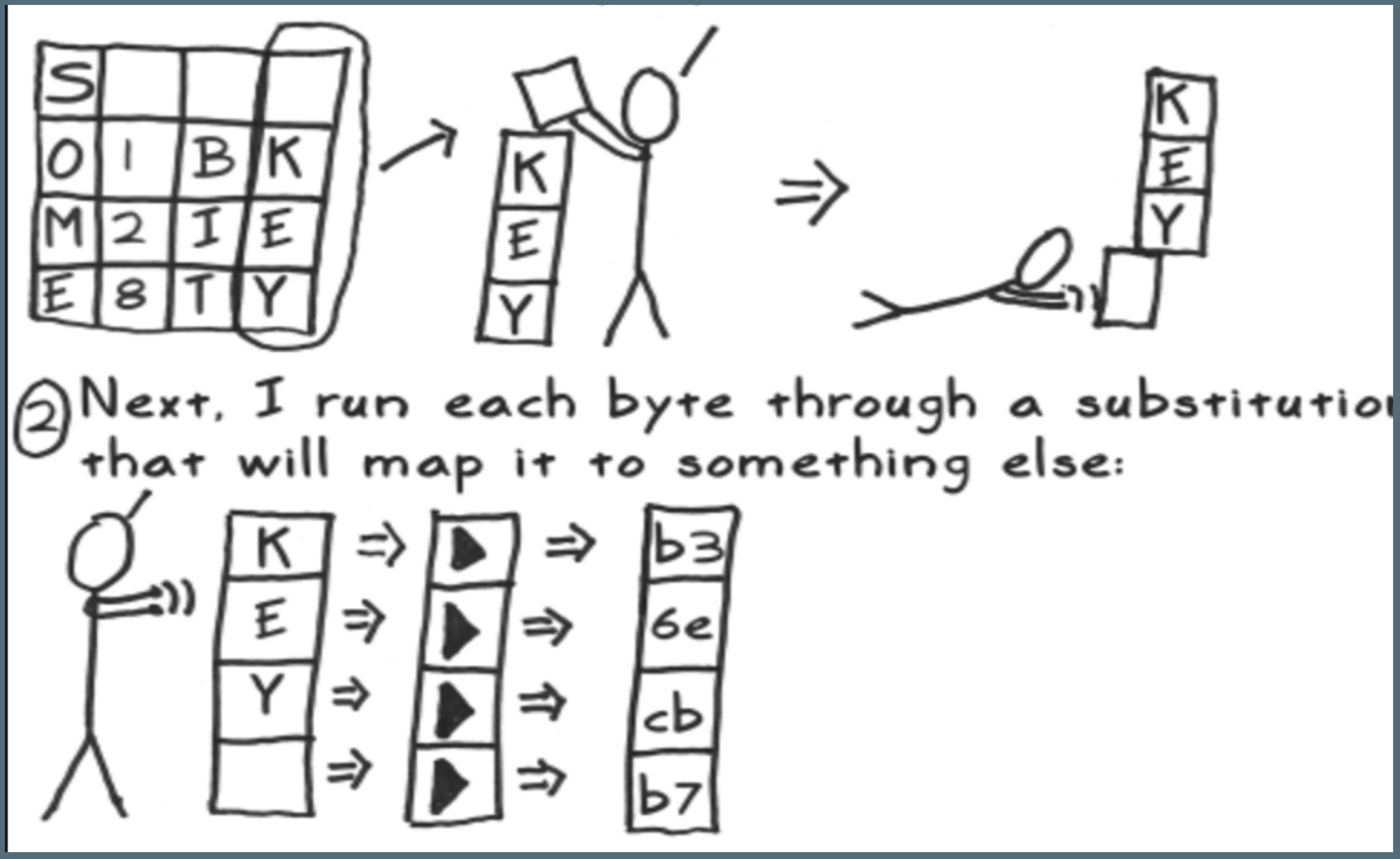


Initial encryption with Key (128bit)

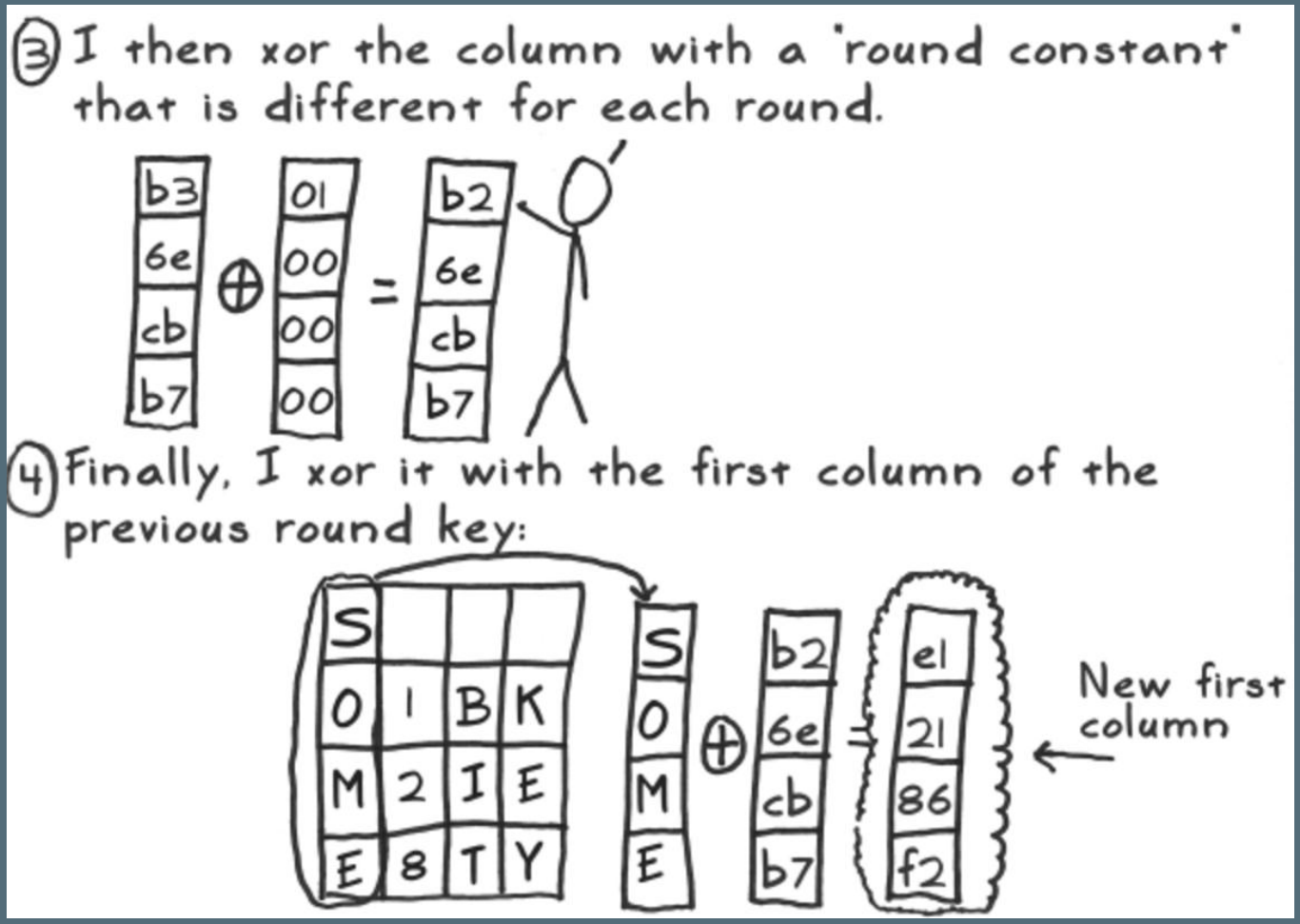
The initial round has me xor each input byte with the corresponding byte of the first round key.



Substitution technique for other keys



Substitution technique for other keys



Hands on Application for AES Encryption

http://aes.online-domain-tools.com/

- Public-Private Key encryption AKA PKI
- Developed by Ron, Shamir and Adleman in 1997.
- Using Public Key and Private key to encrypt and decrypt the messages
- Encrypts using public key and decrypt using private key

- Public-Private Key encryption AKA PKI
- Developed by Ron, Shamir and Adleman in 1997.
- Using Public Key and Private key to encrypt and decrypt the messages
- Encrypts using public key and decrypt using private key

- Choose 2 different prime numbers P,Q
- Calculate Modulus N = P*Q
- Calculate Totient X(N) = (P-1) (Q-1)
- Choose an integer E
  - Should be between 1 and X(N)
  - The GCD (E and X(N) = 1
- Calculate D = 1 + K * X(N) / E

- Prime numbers P =3 ,Q =5
- Calculate Modulus N = P*Q = 15
- Calculate Totient X(N) = (P-1) (Q-1)

X(N) = (2) (4) = 8

- Choose an integer E (Public Key)
  - Random selection that should satisfy:
  - Should be between 1 and X(N) (8)
  - The GCD (E and X(N) = 1
  - Therefore E=7 as its the number
    - Between 1 and 8
    - GCD of E and X(N) is 1

- Calculate D (Private Key)
  - Formula D = 1 + K * X(N) / E
  - K will be a random value starting from 0,1,2…
  - Value of K should be less than the value of E=7
  - The value of k will be changed until the value of equation is an integer and not a fraction
  - Assume K =1
    - 1+1*8/7 = 1+8/7= 9/7 = 1.24
    - 1+2*8/7 = 1+16/7= 17/7 = 2.42
    - 1+6*8/7 = 1+48/7= 49/7 = 7
  - Therefore the value of D = 7

- Encryption:
  - Cipher = C , Message = M = 2
  - C = ((M)^E)mod pq
  - C = ((2)^7) mod 15
  - C= (128) mod 15
  - C=128 mod 77 = 8

- Cipher:

144643602724969572408518703426134340763734522751217526473604641363178576468957263666622253789715319546865369665729385309620153559612800391288241922799461900336928606242039205889723393039751165794039846990733677929842721509238963315892672741118619591414293302621998111792096036946564215946335758619851109875400558930013097528363985642185048929535966504095947703528184165217012834368463658830038592096291421132889989793954497271306896737716409455275151550293862390595050978001174671772916707850220027139523031416788950720013990868784654013468377272128732352273645872702161648443380393764357907694376229619388233504142648252743944924390551560704492709089383951117980259418257445822558139161553644198700654617497841499576869902775844360490456691643285889913393123058971185345090754054059542477677075205229178440023652566600705621281746011894818223044281817138874614763635023450960993983575312156062075089134523100430036429569055865730319563634831414589143605553545057773590087890625

- Mod: 65

- Message M = (C^D) mod PQ
- M = (8^7) mod 15
- M = 2097152 mod 15
- M = 2

- **Prepare a brief write up on the different components of the AES Encryption.**
- **Explain in short the process of encryption in AES.**