TRIPLE DES

Presentation by

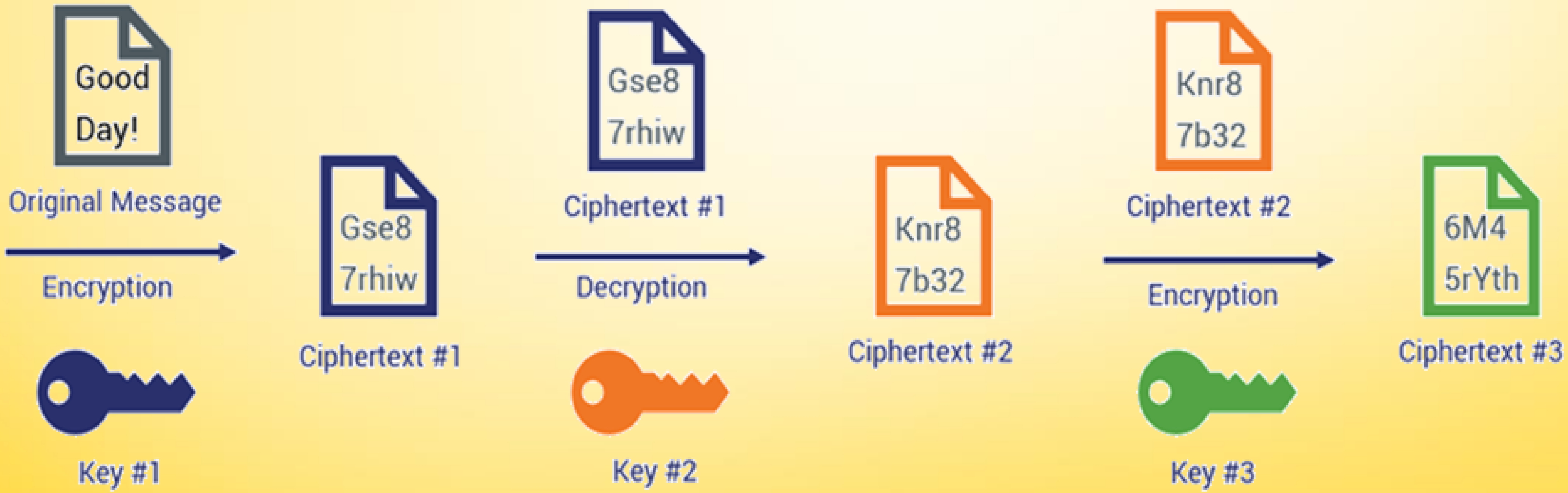
Mr. Tharshan and Mr. Lavan

Algorithm

- Uses a block of size 64 bits.
- It uses three stages of DES for encryption and decryption with three different keys. 3-key 3DES has an effective key length of 168 bits and is defined as,

  C=E(K3,D(K2,E(K1,P)))
  P=D(K1,E(K2,D(K3,C)))

Triple DES


Good Day!
Original Message
Encryption
Key #1
Gse8 7rhiw
Ciphertext #1
Gse8 7rhiw
Ciphertext #1
Decryption
Key #2
Knr8 7b32
Ciphertext #2
Knr8 7b32
Ciphertext #2
Encryption
Key #3
6M4 5rYth
Ciphertext #3

Applications

- The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it .
- Microsoft OneNote and Microsoft Outlook 2007 use Triple DES to password protect user content.
- Firefox and Mozilla Thunderbird use Triple DES in CBC Mode to encrypt website authentication login credentials when using a master password.

Benefits of using 3DES

- With 168-bit key length, it overcomes the vulnerability to brute-force attack of DEA.
- Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES.

Drawbacks

- It has three times as many rounds as DES, is correspondingly slower.
- Uses 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable .
- The National Institute of Standards and Technology (NIST) issued a call for proposals to develop the Advanced Encryption Standard (AES) as a replacement for DES

THANK YOU