School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22

WEEK 3.1

SYMMETRIC KEY CRYPTOSYSTEM

Last Updated: 10/10/2021

Contents

Week 1 & 2 Recap

Crypto Vocabulary

7 security Domains

Classical Cryptography

Modular Arithmetic

Week 1 & 2 Recap

Components Covered

- Skill
- Knowledge
- Thinking
- Activity
- Feedback

Topics Covered

- Crypto Vocabulary
- 7 Security Domains
- Classical Cryptography
  - Transposition Ciphers
    - Scytale
    - Columnar transposition
    - Bifid cipher
    - ADFGX cipher
  - Substitution Ciphers
    - Pigpen cipher
    - Shift cipher
    - Affine cipher
- Modular Arithmetic

Cryptanalysis

Kerckhoffs' principle

Hacker's objective

Attack Models

Statistical Properties of English Language

Cryptanalysis

- Kerckhoffs' principle
  - Hacker knows the cryptosystem being used
- Hacker's objective
  - Determine the KEY
- Why? – Allows the hacker to
  - decrypt any cipher text that is encrypted using the KEY.
- How? – Attack model
  - specifies the information available to the hacker when he mounts his attack.

Common Types of Attack Models

- Cipher text only attack
  - Hacker knows only the cipher text
- Known plain text attack
  - Hacker knows a plain text and its corresponding cipher text
- Chosen plain text attack
  - Hacker can chose the plain text and obtain its corresponding cipher text
- Chosen cipher text attack
  - Hacker can chose the cipher text and obtain its corresponding plain text

Statistical Properties of English Language

- Probabilities of occurrence of 26 letters
- Source:
  - H. Beker and F. Piper, Cipher Systems: The Protection of Communication.

S.N.	Letters (in the order of higher probability of occurrence)	Probability of Occurrence
1	E	0.120
2	T, A, O, I, N, S, H, R	Between 0.09 ~ 0.06
3	D, L	Around 0.04
4	C, U, M, W, F, G, Y, P, B	Between 0.028 ~ 0.015
5	V, K, J, X, Q, Z	Less than 0.01

Decrypt using statistical properties

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Cryptosystem
  - Shift Cipher (with modular arithmetic)
    - CT = (PT + Key) mod 26
    - PT = (CT - Key) mod 26
- Find the "Key" for the below cipher texts
  - CT: UTZNKRKBKR
  - CT: XYWKDDOBSP

Goals of Cryptography

- Confidentiality & Privacy
- Integrity
- Availability
- Authentication
- Non-repudiation

Goals of Cryptography

- Confidentiality & Privacy
  - ensures only authorized parties can view the data
- Integrity
  - ensures data is correct and unaltered
- Availability
  - Authorized users can access data
- Authentication
  - communicating parties can prove their identity to each other
- Non-repudiation
  - proves that a user as indeed performed an action / transaction

Goals of Cryptography

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information
Authenticity	Provides proof of the genuineness of the user	Cryptography can prove that the sender was legitimate and not an imposter
Nonrepudiation	Proves that a user performed an action	Cryptographic nonrepudiation prevents an individual from fraudulently denying they were involved in a transaction

(Source: SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS
4th Edition – Mark Ciampa - Cengage Learning)

Symmetric Key Cryptosystem

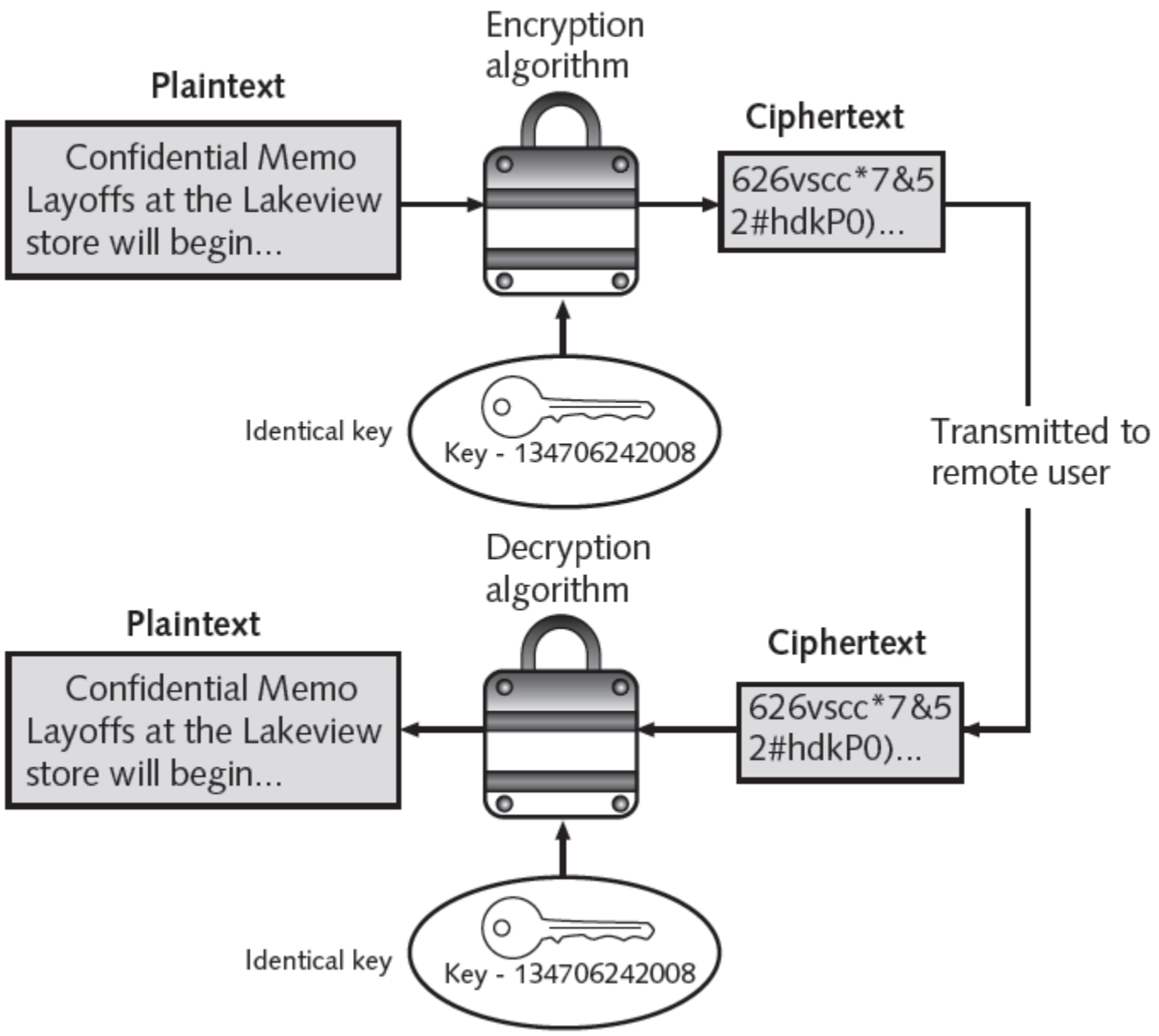
- Product Ciphers
- Concept of Symmetric Key Cryptosystem
- Importance of Key Length
- Stream Cipher
- Block Cipher
- Popular Block Ciphers: 3DES & AES
- Advantages and Disadvantages of Symmetric Key Cryptosystem

Product Ciphers

- Most classical cryptosystems could be broken via
  - Exhaustive key search or brute force
  - Frequency analysis or statistical properties of the language
- Therefore in 1949 Claude Shannon presented the concept of
  - Product Cipher
    - combines a sequence of substitution, permutation (transposition), and modular arithmetic
- Symmetric Key Cryptosystem is a product cipher

Symmetric Key Cryptosystem

Same shared key used to encrypt and decrypt data



(Source: SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS 4th Edition – Mark Ciampa - Cengage Learning)

Importance of Key Length

- To secure the data, we need to secure the key.
- Given a specified key length, the number of keys that must be tried (using Brute Force Attack) to exhaust all possibilities are shown on the next slide:

Importance of Key Length

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Key combinations versus Key size

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Time to crack Cryptographic Key with Supercomputer

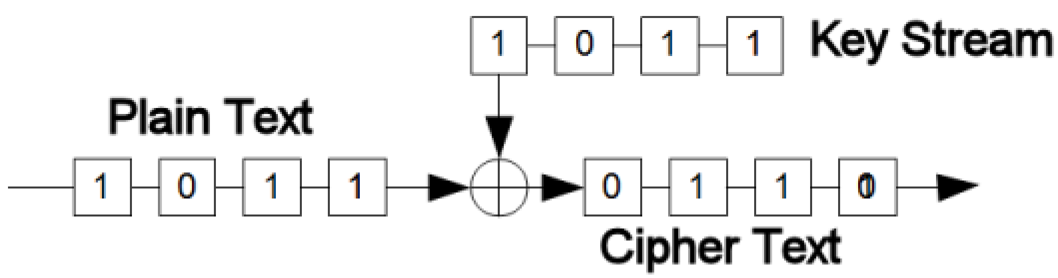
Source: http://www.eetimes.com/document.asp?doc_id=1279619
How secure is AES against brute force attacks?

2 Types of Symmetric Key Cryptosystems

- Based on amount of data to be processed at a time, symmetric key cryptosystems are divided into 2 types
  - Stream Cipher
    - Each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. [Source: http://en.wikipedia.org/wiki/Product_cipher]
  - Block Cipher
    - Works on entire block of plaintext at a time
    - Separate blocks of 8 to 16 bytes encrypted independently

Stream Cipher

- Encrypt data one bit at a time as they become available.
- Stream ciphers
  - execute at a higher speed than block ciphers
  - have lower hardware complexity
  - stream ciphers can be susceptible to serious security problems if used incorrectly

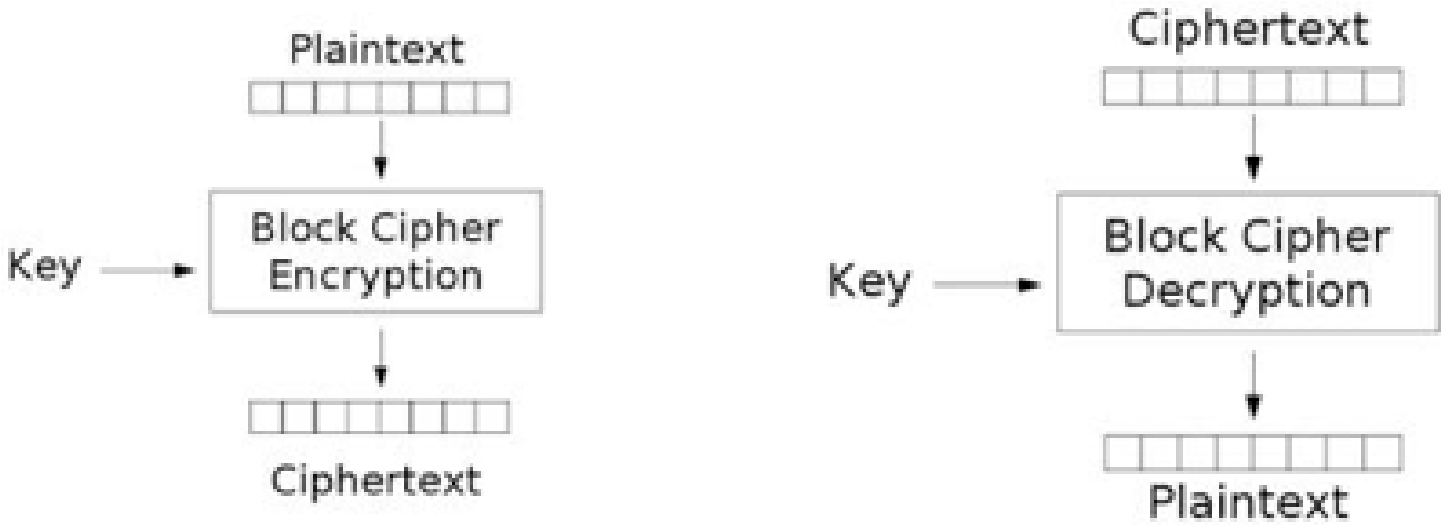


Source: https://hyperploid.blogspot.com/2010/08/digital-ciphers.html

Source: http://en.wikipedia.org/wiki/Product_cipher]

Block Cipher

- Encrypt data one block at a time.
- Block ciphers considered more secure because output is more random



Source: http://wdict.net/word/block+cipher/

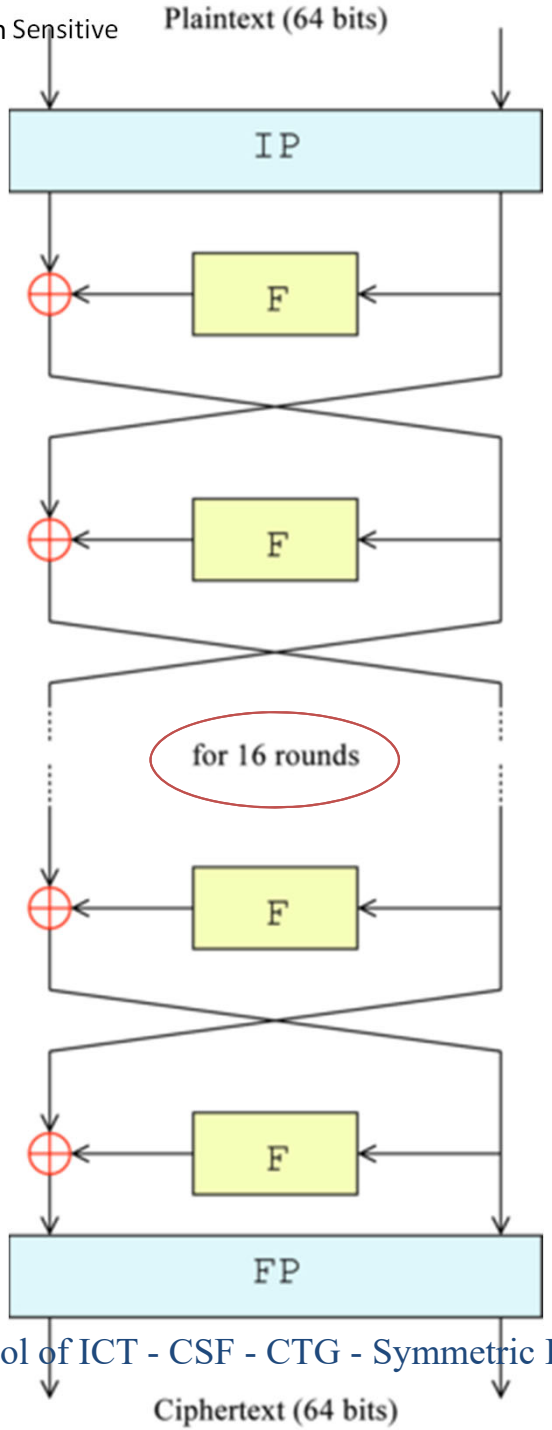
Popular Block Ciphers

- 3DES
  - Triple Data Encryption Standard
- AES
  - Advanced Encryption Standard

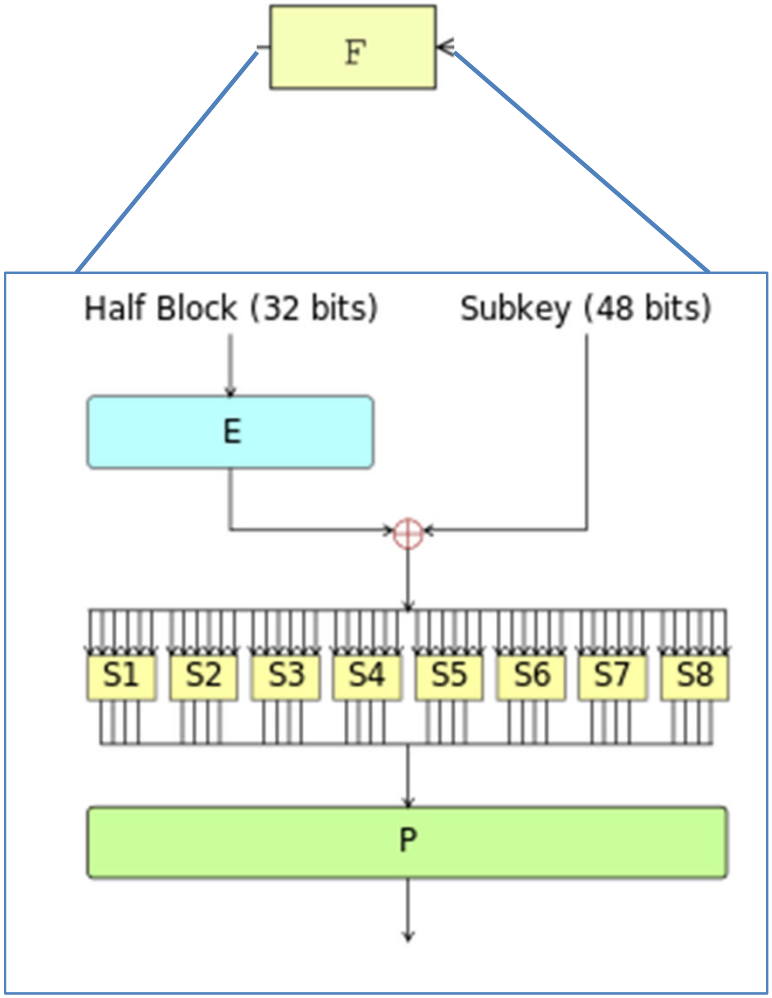
3DES

- Data Encryption Standard (DES)
  - Based on product originally designed in early 1970s
  - Adopted as a standard by the U.S. government
  - Key size only 56bits
  - It was first broken in the year 1997
  - In Jan 1999 a DES key was broken in 22 hours and 15 minutes.
- Triple Data Encryption standard (3DES)
  - Designed to replace DES
  - Uses three rounds of encryption
  - Cipher text of first round becomes input for second iteration

DES

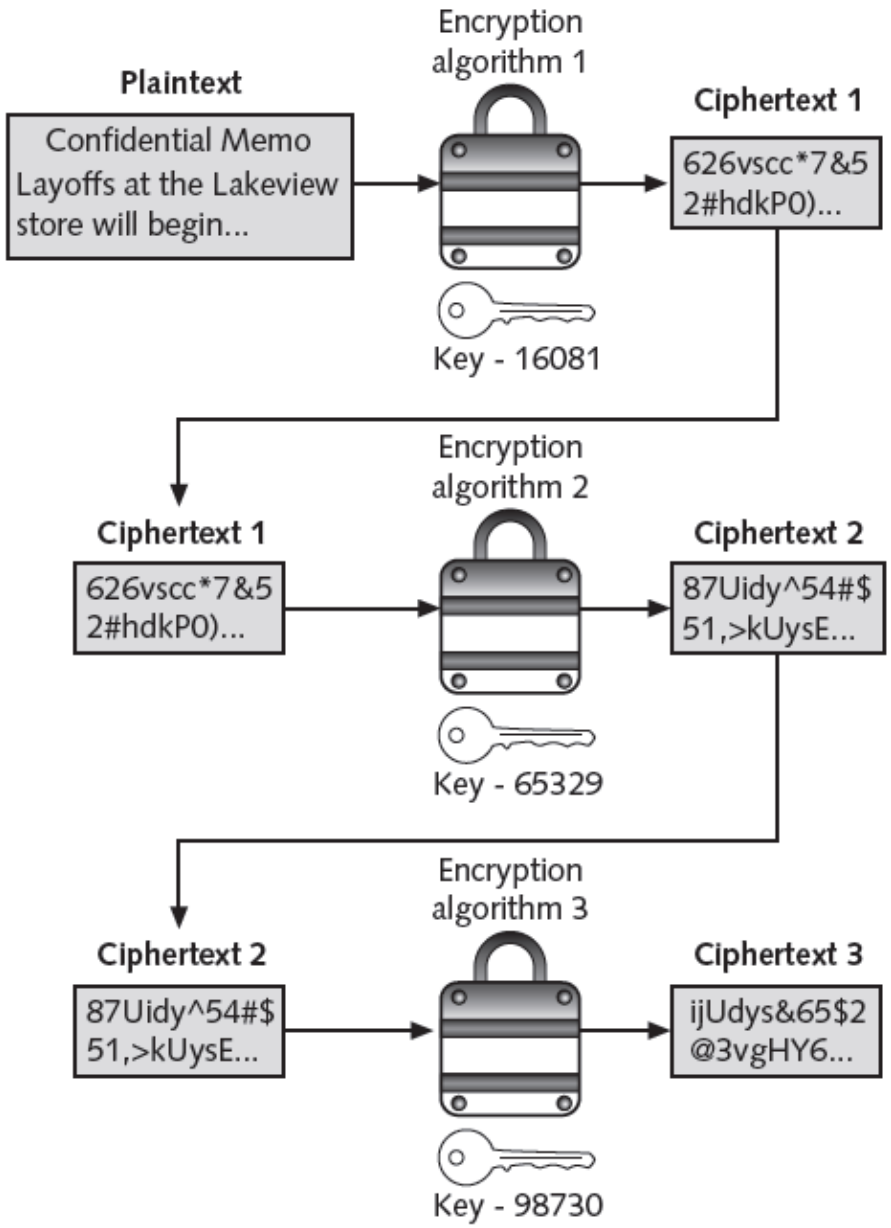


The Feistel function (F-function) of DES



IP: Initial Permutation
FP: Final Permutation
S1 – S8: Substitution Boxes (S-box)
P – Permutation Box (P-box)

3DES

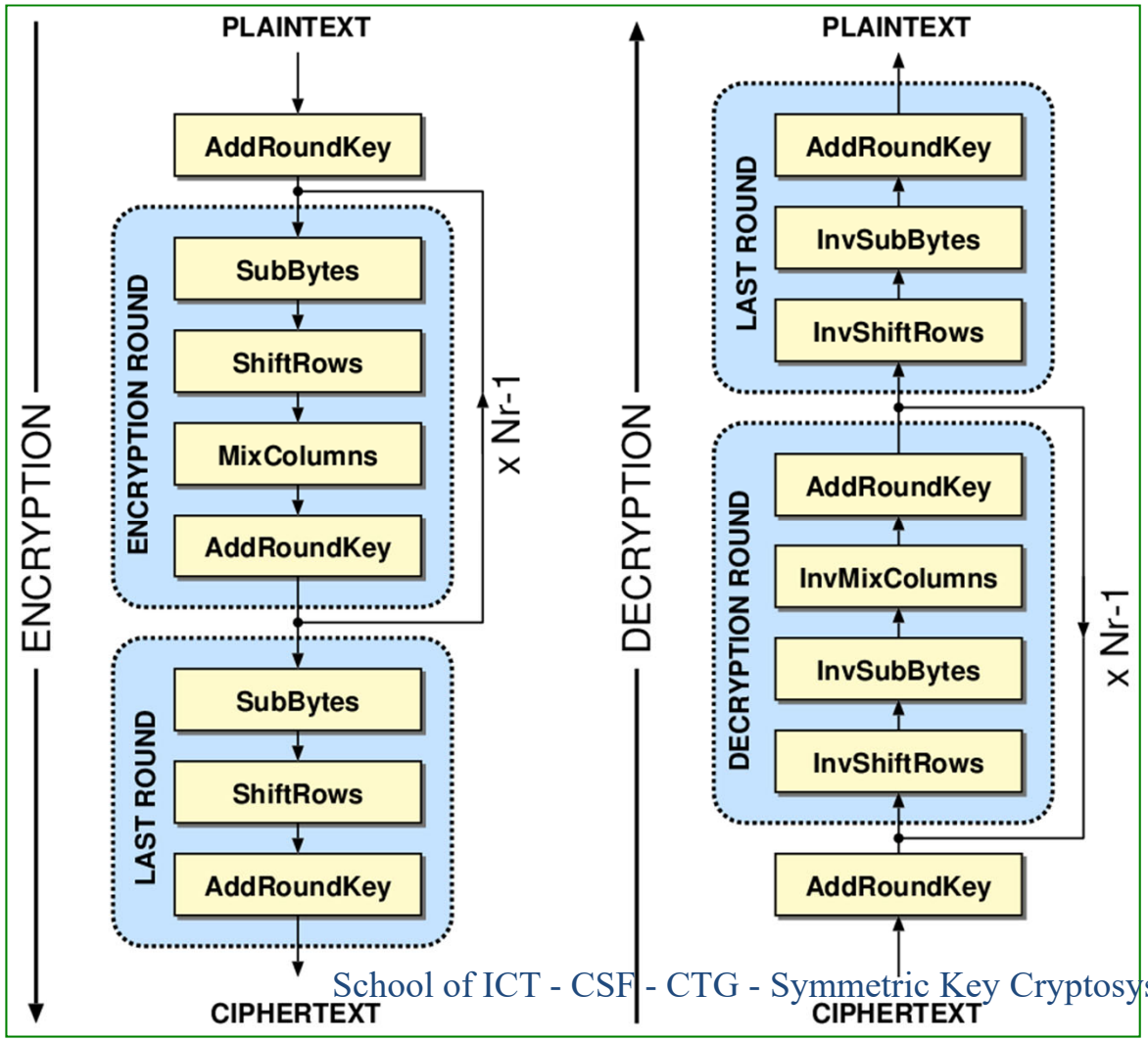


(Source: SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS
4th Edition – Mark Ciampa - Cengage Learning)

AES (1/2)

- Advanced Encryption Standard (AES)
  - Symmetric cipher approved by NIST in 2000 as replacement for DES
  - Official encryption standard used by the U.S. government
  - Performs three steps on every block of plaintext
  - Designed to be secure well into the future

AES (2/2)



10 cycles of repetition for 128-bit keys.
12 cycles of repetition for 192-bit keys.
14 cycles of repetition for 256-bit keys.

Source:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Comparison between AES, 3DES and DES

Factors	AES	3DES	DES
Key length	128, 192 or 256 bits	(k1, k2 and k3) 168 bits (k1 and k2 are same) 112 bits	56-bit
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block size	128, 192, or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential; Brute Force Attacker could analyze plain text using differential cryptanalysis	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	One only weakness, which exists in DES	Proven inadequate
Possible keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5 x 10^{21} years	For a 112-bit key: 800 days	For a 56-bit key: 400 days

Source: Alanizi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Advantages and Disadvantages of Symmetric Key Cryptosystems

- Advantages
  - Extremely secure
  - Relatively fast
    - Due to simple substitution, permutation (transposition), and modular arithmetic operations
- Disadvantages
  - Key distribution
    - Requires a secure communication channel to share key between parties
  - Key management
    - Each party have to maintain a unique shared key with every other communicating party
    - If “n” is the number of parties in a group, who want to use symmetric key cryptosystem
      - Then the total number of keys required for the group would be: n x (n -1) / 2

Tools for Data Encryption Part 1

KeePass

AES Crypt

Steg

7-Zip

Objective

- As ISF students you'll find these tools very important
- These tools allow you to make it a habit to
  - use strong passwords
  - encrypt important files
  - securely communicate with peers
- These tools will lead you to better understand Symmetric Key Cryptosystems

Activity 3.1

- Install and explore the tools listed below
  - KeePass
    - http://keepass.info/
    - Use Professional Edition
  - AES Crypt
    - https://www.aescrypt.com/
    - Double click on "AESCrypt.msi" to install
  - Steg
    - http://www.fabionet.org/
    - Use only the PassPhrase symmetric cryptography feature
  - 7-Zip
    - http://www.7-zip.org/
    - Use the 7z format with encryption

Summary (1/3)

- Cryptanalysis
  - Kerckhoffs' principle
  - Hacker's objective
  - Attack Models
  - Statistical Properties of English Language
- Goals of Cryptography
  - Confidentiality & Privacy
  - Integrity
  - Availability
  - Authentication
  - Non-repudiation

Summary (2/3)

- Symmetric Key Cryptosystem
  - Product Ciphers
  - Concept of Symmetric Key Cryptosystem
  - Importance of Key Length
  - Stream Cipher
  - Block Cipher
  - Popular Block Ciphers: 3DES & AES
  - Advantages and Disadvantages of Symmetric Key Cryptosystem

Summary (3/3)

Component	You learnt
Thinking	Kerckhoffs' principle Common Types of Attack Models Advantages and Disadvantages of Symmetric Key Cryptosystems
Skill	Decrypt using statistical properties Tools for data encryption
Activity	Decrypt using statistical properties
Knowledge	Goals of Cryptography Stream Cipher Block Cipher
Feedback	Decrypt using statistical properties Kerckhoffs' principle Common Types of Attack Models Advantages and Disadvantages of Symmetric Key Cryptosystems