Live Session 03

Symmetric Key Cryptography

CS 7349

Spring 2024

World Changers Shaped Here

SMU

© Shaibal Chakrabarty

Contents

- Security News of the Week
- House Keeping
- Class Presentation – Special Topic
- Concepts: Security Fundamentals
- Block ciphers

Sources: YouTube/Dr. Dan Boneh, Cryptography 1; www.simonsingh.net; Cryptography and Network Security, William Stallings; schneier.com

House Keeping

- Status of Teams for Term Paper? Topic?
- Term Paper Topic, team, due by 01/28/2024; Checkpoint on 01/29, 01/3
- Quiz 1 and Homework 1 are issued
- Quiz 1, 1 week; Homework 1, 2 weeks
- Presentations start 01/22/2024

Security News of the Week – Spring 2024

- https://arstechnica.com/security/2024/01/mass-exploitation-of-ivanti-vpns-is-infecting-networks-around-the-globe/
  - Ivanti VPNs worldwide have been compromised. Several government agencies impacted (Cloud providers own this VPN box. CISA directive)
- https://www.reuters.com/technology/cybersecurity/us-secs-x-account-hacked-with-sim-swapping-agency-says-2024-01-22/
  - “SIM swapping” hacked SECs X-account to release fake bitcoin news
- https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/
  - “Mother of all breaches”: 26B records, 12TB of data from multiple hacks

Source: arstechnica.com, reuters.com, cybernews.com

New Urban Dictionary terms

- SIM swapping
- Doxxing
- Swatting

Other

- Naughty – bypassing the system
  - https://en.wikipedia.org/wiki/Sci-Hub
  - 2011 khazakh grad student launches sci-hub.io and now sci-hub.cc to protest against paywalled research.
  - Considered illegal and site banned after lawsuit by Elsevier. Still exists
- Nice – opensource libraries
  - Keyczar/K2: an opensource crypto toolkit released by Google in 2008
  - https://security.googleblog.com/2008/08/keyczar-safe-and-simple-cryptography.html

CS 7349 – Tying it all together

INTRODUCTION TO CS7349 AND THE THREAT LANDSCAPE	HASH FUNCTIONS	NETWORK SECURITY
INTRODUCTION TO NETWORKS	MESSAGE AUTHENTICATION CODES	SECURITY – CLOUD, WIRELESS/5G, DDoS, SASE, IoT, SDN, Smart Cities
SYMMETRIC KEY CRYPTO	KEY MANAGEMENT	FRAMEWORKS, STANDARDS, OPERATIONS, Governance/Risk/Compliance
USING SYMMETRIC KEY CIPHERS	IDENTITY AND ACCESS MANAGEMENT	REVIEW/ADDITIONAL TOPICS
RANDOMNESS AND PSEUDORANDOM NUMBERS		
PUBLIC KEY CRYPTO/Team Paper		

Confidentiality **Integrity** **Availability** **Networks/Application**

Spring schedule

Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

Class Presentation - Special Topic

- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - Adu, Aliliele, Blocker, Braden, Brown, Burnett…

Project Timeline (For 9 page paper)

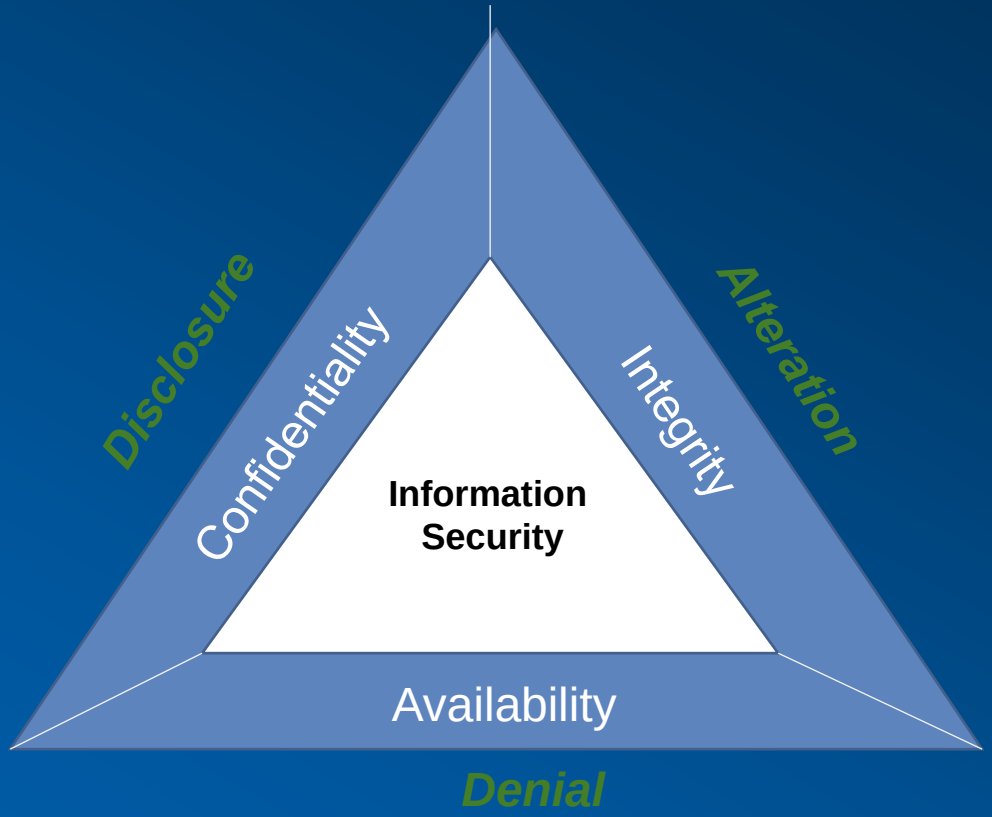
- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

A LaTex template and example paper will be provided

Project – 1st deliverable

- Team projects (3 per team)
- Choose topic (from topic list or your own)*
- Within topic, identify problem to be addressed (no survey projects, only problem solving projects - survey is a part of your problem solution and is contained in the final paper)
- Confirm problem with professor

InfoSec, CIA, Threats



Source: “Information Security Illuminated”, Solomon and Chapple, 2005, Sudbury, MA:Jones and Bartlett.

Network Security Basics

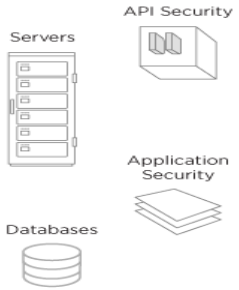
The IT Security Chain

upwork™

The more links in your network's chain—databases, cloud-based servers, APIs, and mobile applications—the more potential vulnerabilities you face. Here's an overview of areas of IT security to consider.

IT Security

NETWORK SECURITY



- Security Engineering
- Vulnerability Testing
- Penetration Testing
- Network Intrusion Detection Systems (NIDS)
- Firewalls

INTERNET SECURITY

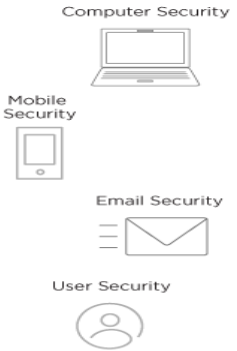
- HTTPS
- SSL Certificates
- OAuth 2.0

CLOUD SECURITY

- OAuth 2.0
- Web Sockets

WIRELESS SECURITY

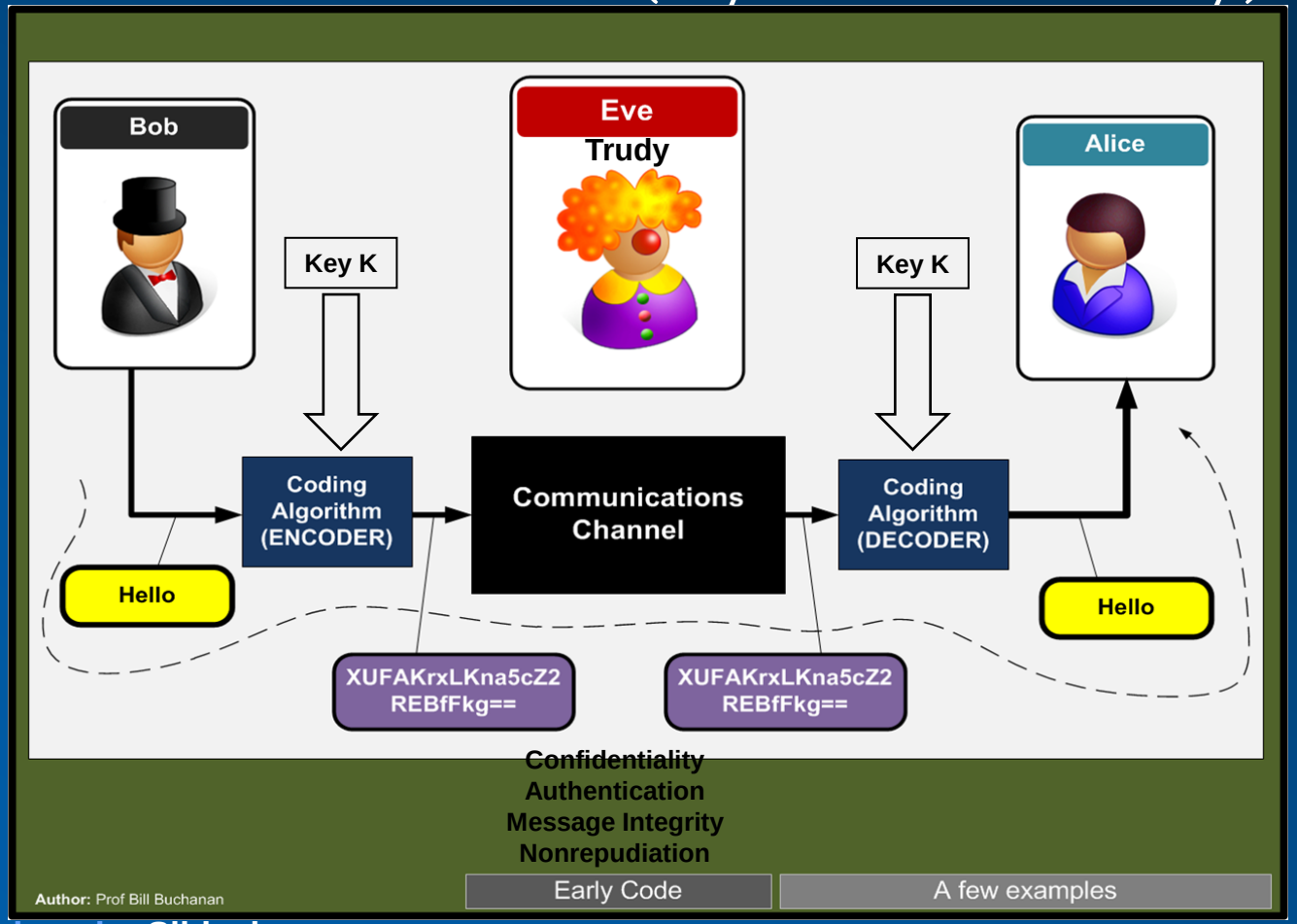
END POINT SECURITY



- VPNs
- Encryption
- Anti-Malware

Source: Upwork Global, Inc

Secure Communication (Symmetric Key)



Source: bill@napier.edu; Slideshare

Cryptography Terms

Encryption: the processing of converting a message into an unreadable form

Plaintext: the original (unencrypted) message

Ciphertext: the encrypted or encoded message resulting from encryption

Algorithm (Cipher): a mathematical formula used to convert an unencrypted message into an encrypted message

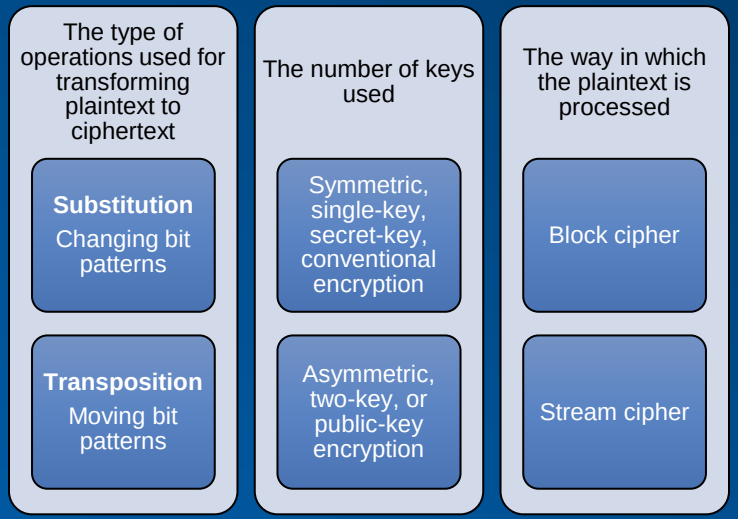
Key: a random and secret value placed within the algorithm to encrypt the plaintext and/or decrypt the ciphertext

Cryptosystem: a computer-based system that provides the four basic objectives of secure communication

Encipher: to encrypt or convert plaintext to ciphertext

Decipher: to decrypt or convert ciphertext back to plaintext

Crypto basics – models and attacks



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Brute-force attack

- **Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained**
- **On average, half of all possible keys must be tried to achieve success**

Cryptanalysis

- **Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext**
- **Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used**

Key Concepts – Crypto basics

- Symmetric Key Crypto
  - 1 key for both E and D
  - Stream and Block
  - Substitution and Permutation
- Substitution Ciphers: Caesar, Monoalphabetic, Playfair, Hill, Polyalphabetic
- One-time PAD (unconditionally secure system)
  - Perfect secrecy (CT gives NO information on PT)
  - Cannot use 3 times!!
  - PT and CT can give key (k = PT (XOR) CT)
  - Random key; k size = m size
- http://www.simonsingh.net/The_Black_Chamber/chamberguide.html ; ex. Monoalpha, Vignere square
- Permutation Ciphers: Rail Fence, Row Transposition, ROTOR Machines (WW2, Enigma, the basis for DES Block cipher)

Game Time! – Build your own cipher

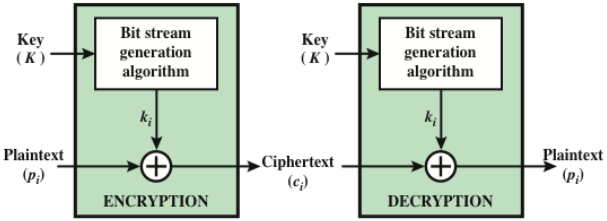
- Meet me at the Toga Party = Plaintext
- Substitution, Transposition
  - Provide Key if necessary
- Demonstrate E and D by hand
- Post your results on the breakout wall and the course wall

Block Ciphers

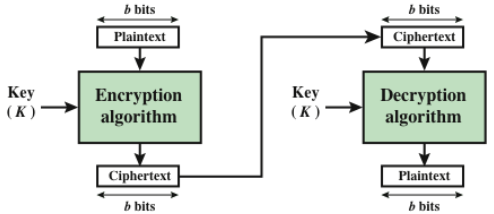
- Feistel Block Cipher, Data Encryption Standard (DES).
- Advanced Encryption Standard (AES), 3DES (triple DES) - later
- An introduction DES by Dr. Dan Boneh
- https://www.coursera.org/learn/crypto/lecture/TzBaf/the-data-encryption-standard
- Communication Theory of Secrecy Systems by Claude Elwood Shannon http://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/Communication_Theory_of_Secrecy_Systems.pdf
- RANDOMNESS!!; Diffusion and Confusion; Avalanche

Review – Block, Stream and DES

- Block Cipher Design and Block Ciphers
  - # of rounds (round functions)
  - Design of the function F (invertible function)
  - Key scheduling algorithm
- Stream Cipher
  - Keystream
- DES
  - Block cipher (feistel block)
  - Now replaced with 3DES/AES



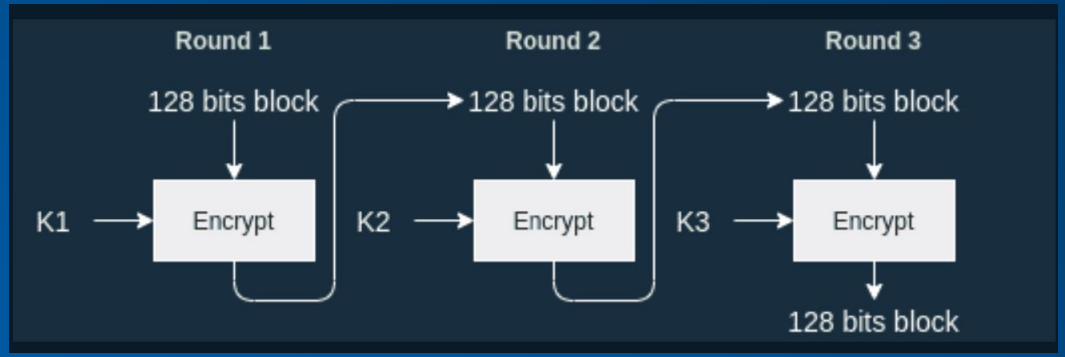
(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

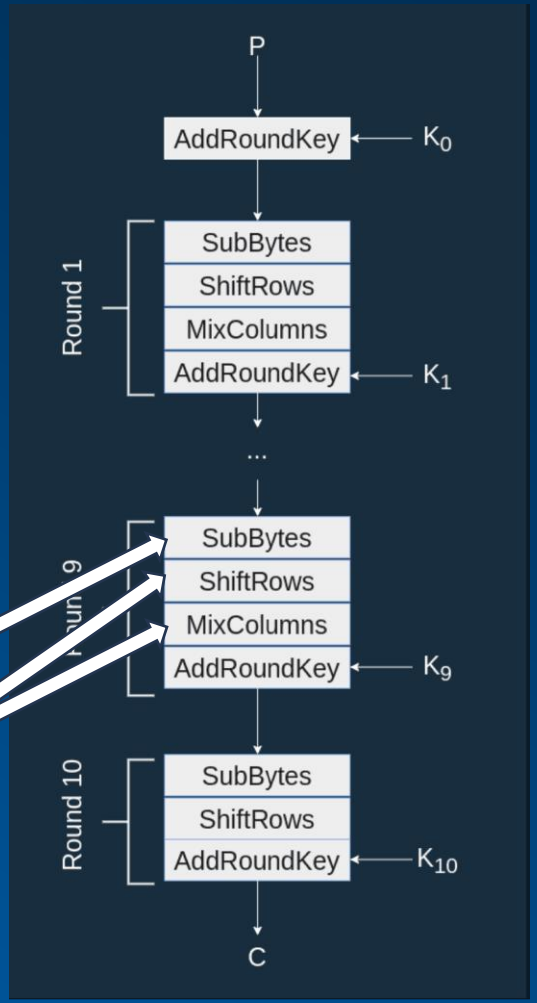
Figure 4.1 Stream Cipher and Block Cipher

Block Ciphers



Substitution

Permutation



Source: https://braincoke.fr/blog/2020/08/the-aes-encryption-algorithm-explained/#aes-in-summary

Unit Overview

- Burning questions?
- Why XOR?
  - Simple gate
  - Reversible for both E and D
  - IF an independent random variable R1 is XORed with a random variable R2 the result is a random variable with uniform distribution (output randomized)

Using Symmetric Key Ciphers

CS 7349

Fall 2023

World Changers Shaped Here

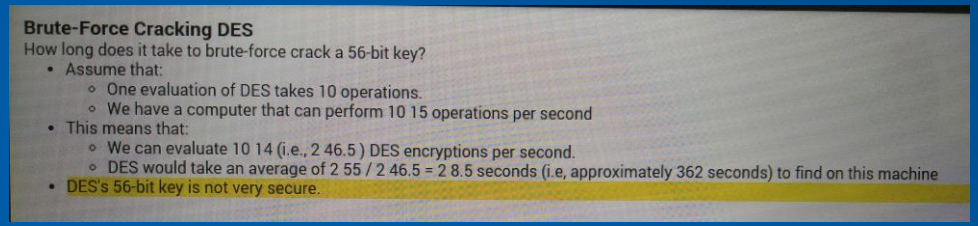
SMU

Wireshark basics

- https://www.youtube.com/watch?v=TkCSr30UojM – Wireshark basics
- https://www.lifewire.com/wireshark-tutorial-4143298 - ‘complete’ tutorial
- https://www.concise-courses.com/security/wireshark-basics/
- http://www.computerweekly.com/tutorial/Quick-and-dirty-Wireshark-tutorial
- https://cs.gmu.edu/~astavrou/courses/ISA_674_F12/Wireshark-Tutorial.pdf
- https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html - from Wireshark.org

Unit Overview

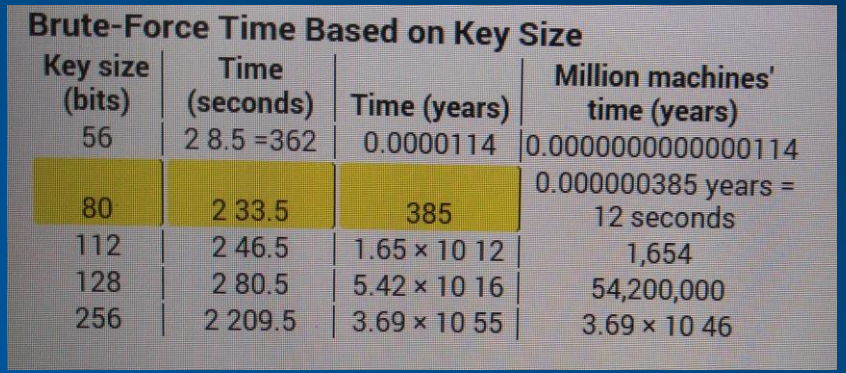
- Burning questions? Anything unusual in Unit 4?
- #1 security criteria for symmetric key cipher?
  - https://www.keylength.com/en/2/



Brute-Force Cracking DES

How long does it take to brute-force crack a 56-bit key?

- Assume that:
  - One evaluation of DES takes 10 operations.
  - We have a computer that can perform 10 15 operations per second
- This means that:
  - We can evaluate 10 14 (i.e., 2 46.5) DES encryptions per second.
  - DES would take an average of 2 55 / 2 46.5 = 2 8.5 seconds (i.e, approximately 362 seconds) to find on this machine
- DES's 56-bit key is not very secure.

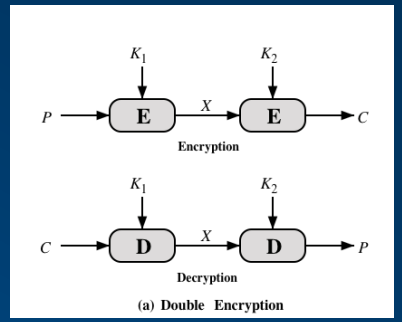


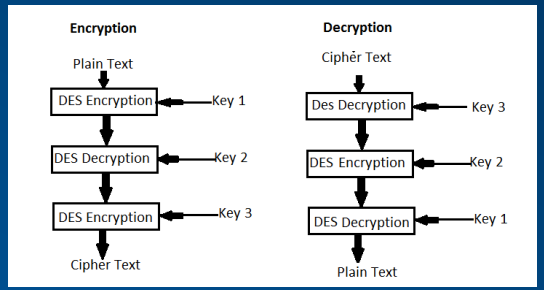
Brute-Force Time Based on Key Size

Key size (bits)	Time (seconds)	Time (years)	Million machines' time (years)
56	2 8.5 =362	0.0000114	0.0000000000000114
80	2 33.5	385	0.000000385 years = 12 seconds
112	2 46.5	1.65 × 10 12	1,654
128	2 80.5	5.42 × 10 16	54,200,000
256	2 209.5	3.69 × 10 55	3.69 × 10 46

Unit Overview – 2DES, 3DES

- DES : brute force attack only 56-bit key
- 2DES : MITM (meet-in-the-middle) attack
  - Brute force ALL encryptions with k1 (get CTi)
  - Brute force ALL decryptions with k2 (get CTj)
  - When CTi = CTj, then the 2 DES keys are k1 and k2!
- 3DES : 2 keys (k1,k2,k1) or 3 keys (k1,k2,k3)
  - 3 independent keys recommended
  - Backwards compatible with DES

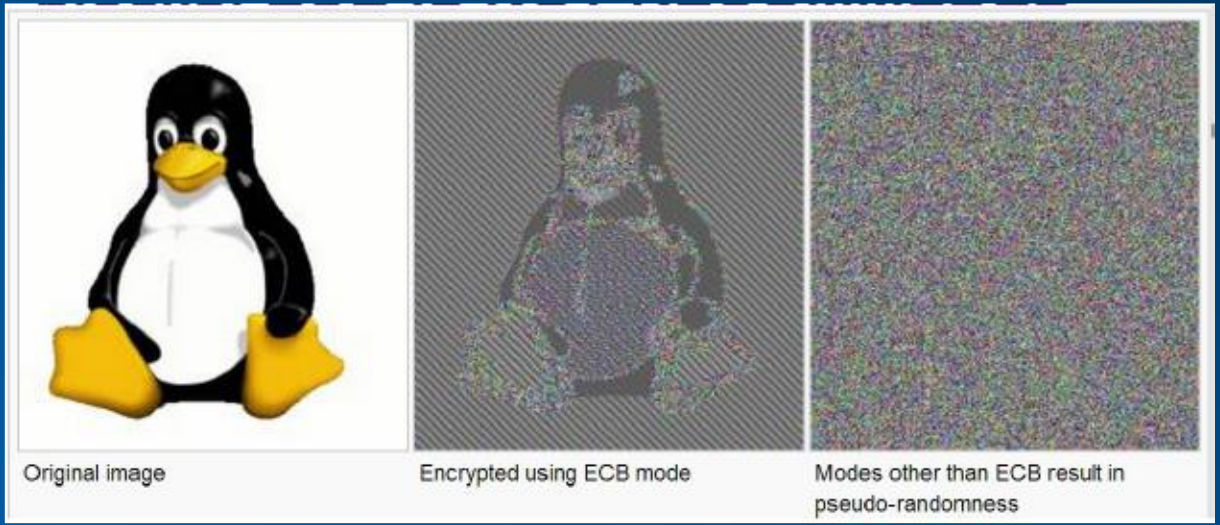




Game Time! – Modes of Operation

- https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
- Group 1 = CBC 10110101111000011010101011010111100011010100 1
- Group 2 = CFB
- Group 3 = CTR
- Group 4 = OFB
- Pro's cons; apps; parallel operations?; bit corruption
- Post your results
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf (NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation)
- XTS-AES is SP800-38E https://csrc.nist.gov/publications/detail/sp/800-38e/final

Modes of Operation



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

AES Block Cipher

- An introduction AES by Dr. Dan Boneh (4:30 mins)
  - https://www.coursera.org/learn/crypto/lecture/cHOMl/the-aes-block-cipher
- The Design of Rijndael, AES – The Advanced Encryption Standard by J. Daemen; V. Rijmen
  - https://dl.acm.org/citation.cfm?id=560131

Thank You!

World Changers
Shaped Here

SMU®

Project Reports

- **Use the LaTex template** provided for your project paper submissions.
- **Read** the Sample paper and **follow** its directions as appropriate in writing your paper.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents.
- https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)

Project Abstract and Intro

- **Abstract** structure (100 word limit for 6 pages)
  - start with statement of what is presented
  - motivate the problem
  - discuss details of what is done at a high level
  - state the main conclusions
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper
  - state the outline for the rest of the paper
    - Conclusions are not stated in the introduction.

Project Paper

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 9 pages exactly. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/read/brpdfvsxsjww#8886a4 ←Paper template