CPS3232

Applied Cryptography

Lecture 1: Introduction and Course Overview

Joseph Bugeja

About Me

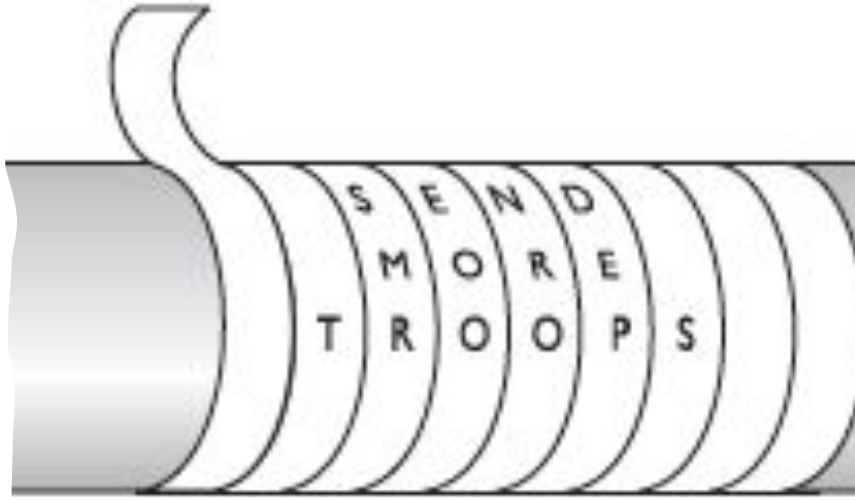
- Course responsible and lecturer
- Ph.D. and postdoc in Computer Science, and MSc in Information Security
- 15+ years of software industry experience (cyber security, development, consultancy, etc.)

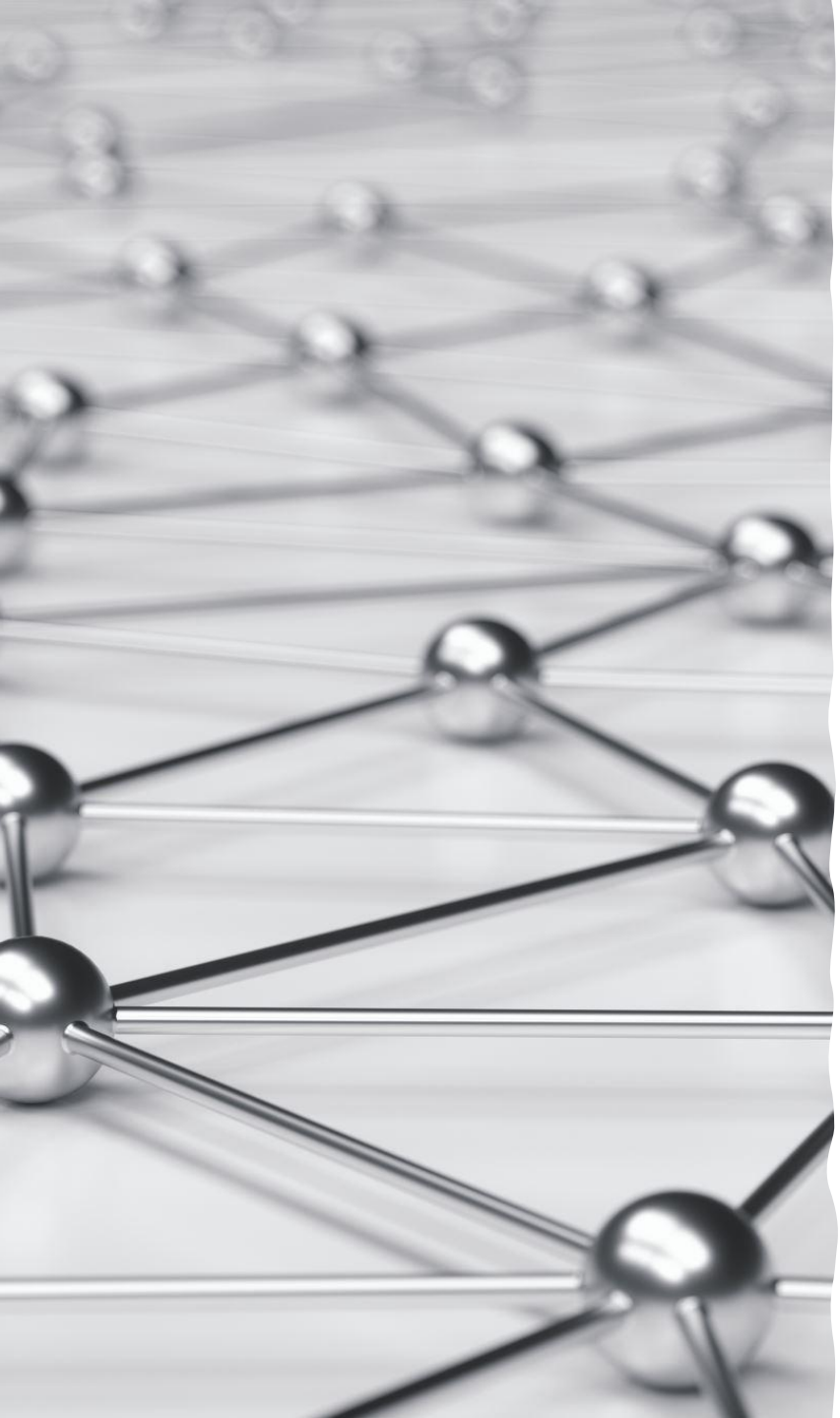
Learning Objectives

- Define cryptology and its types
- Explain the security services provided by cryptography
- Describe and analyze a few historical ciphers
- Identify and describe the differences between different types of attacks against ciphers
- Explain the general objectives and structure of the course, and expectations

Historical Ciphers

- Early signs of encryption in Egypt in ca. 2000 B.C.
- Historical ciphers include the Caesar cipher, Vigenère cipher, and Playfair cipher.
- Modern cryptographic systems are much more secure than historical ciphers.





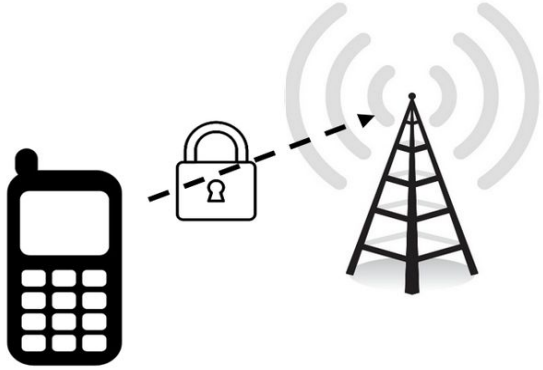
What is Cryptography?

- *Cryptography* is the practice and study of techniques for secure communication in the presence of adversaries.
- *Applied cryptography* focuses on a subset of cryptographic constructions already practical and integrated into larger systems.

Applications of Cryptography

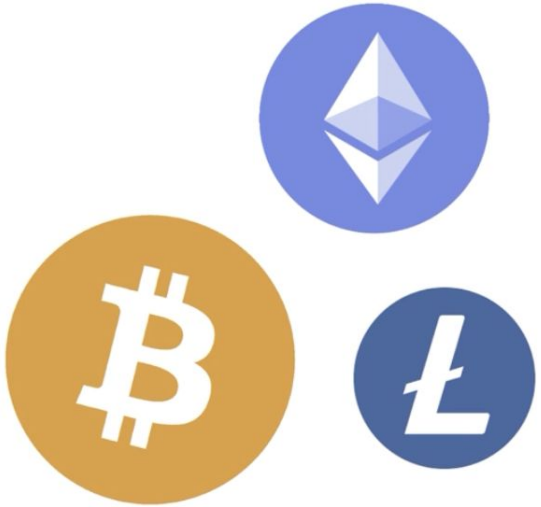
The Enigma Machine being used to secure radio communications during WWII

Secure online payments



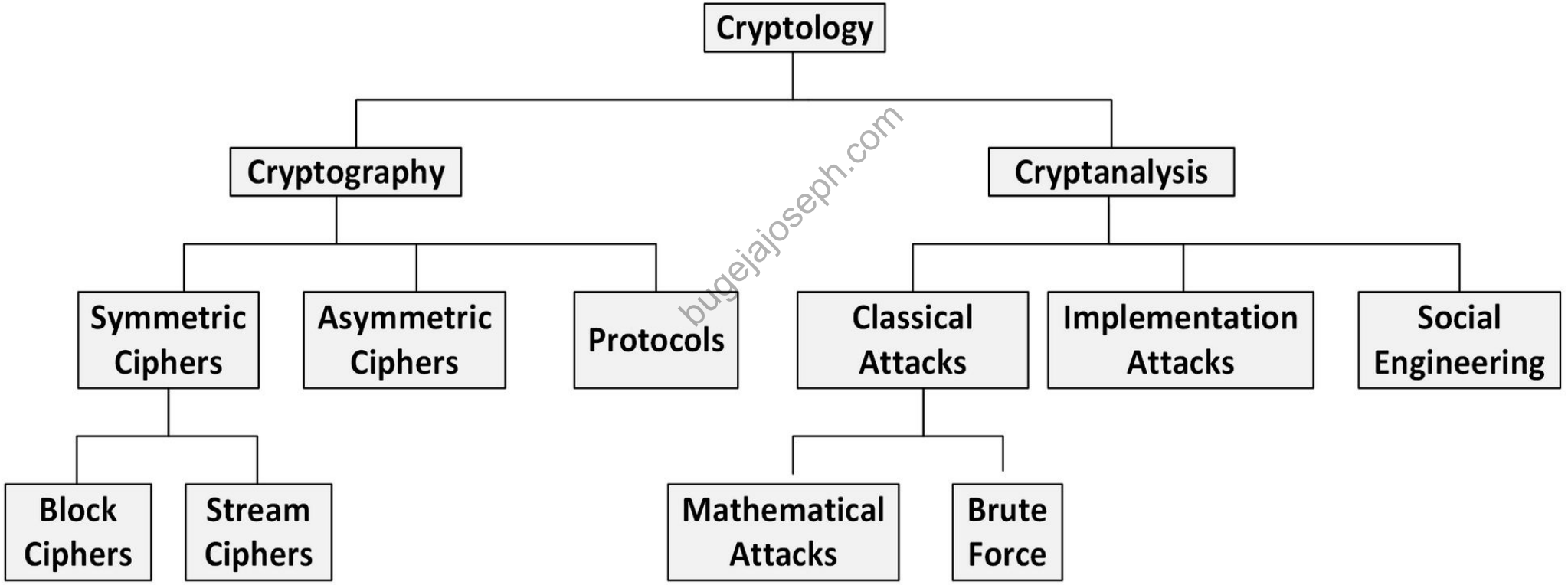
Social media posts

Can you think of other everyday applications of cryptography?



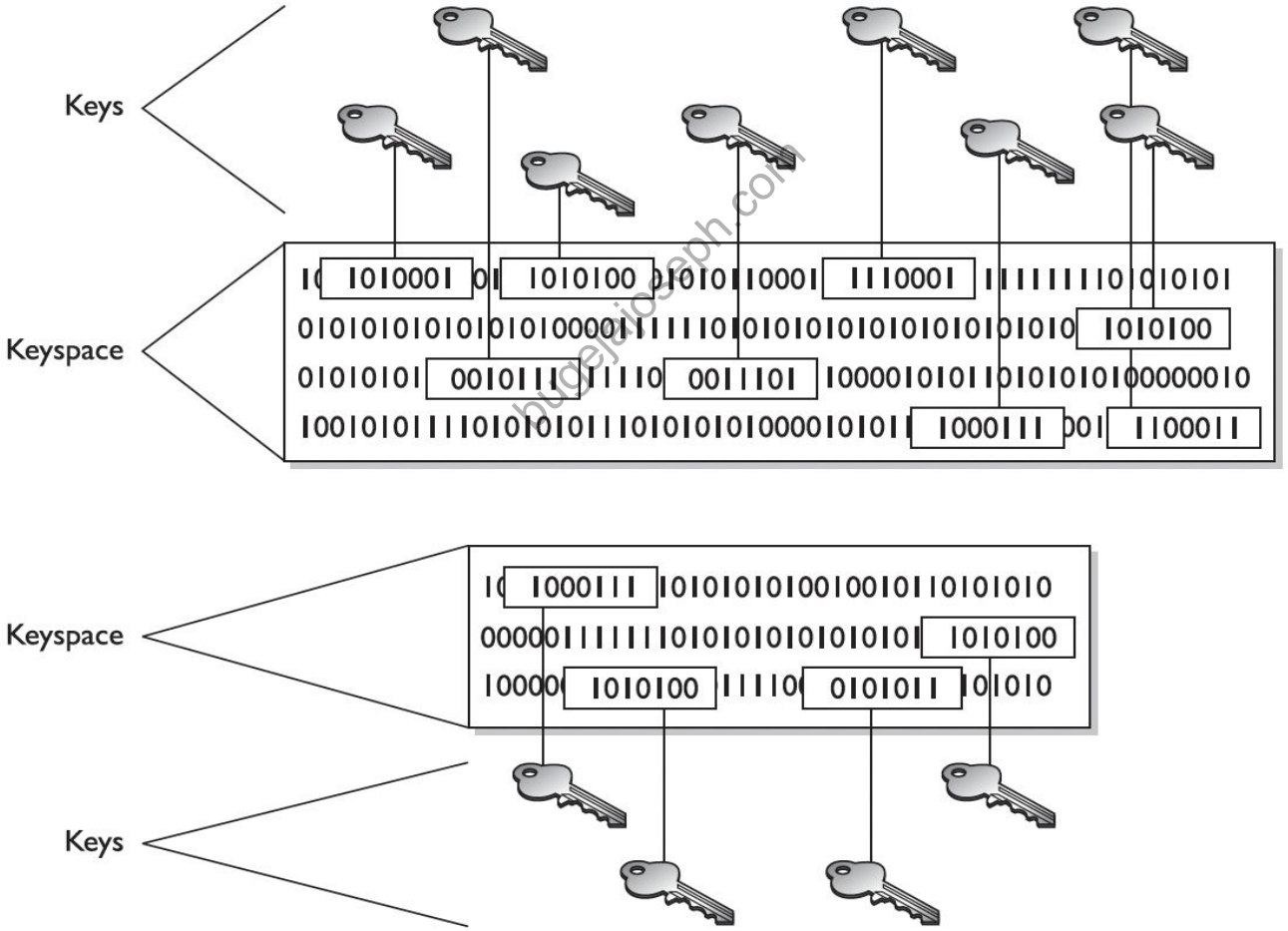
Cryptocurrencies

Overview of the Field of Cryptology



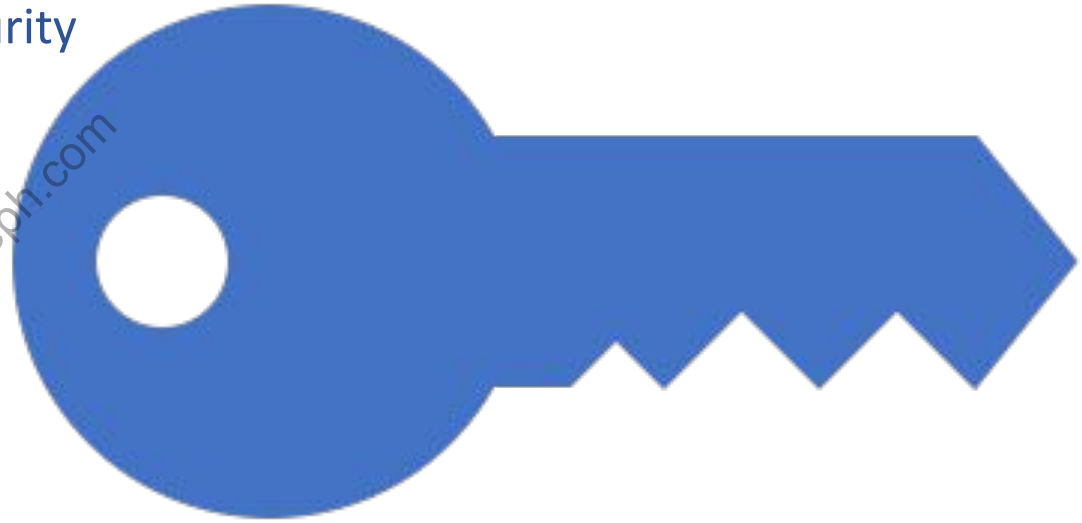
Keys and Keyspace

- A large keyspace allows for more possible keys, e.g., a key size of 512 bits would provide a keyspace of 2^{512}.

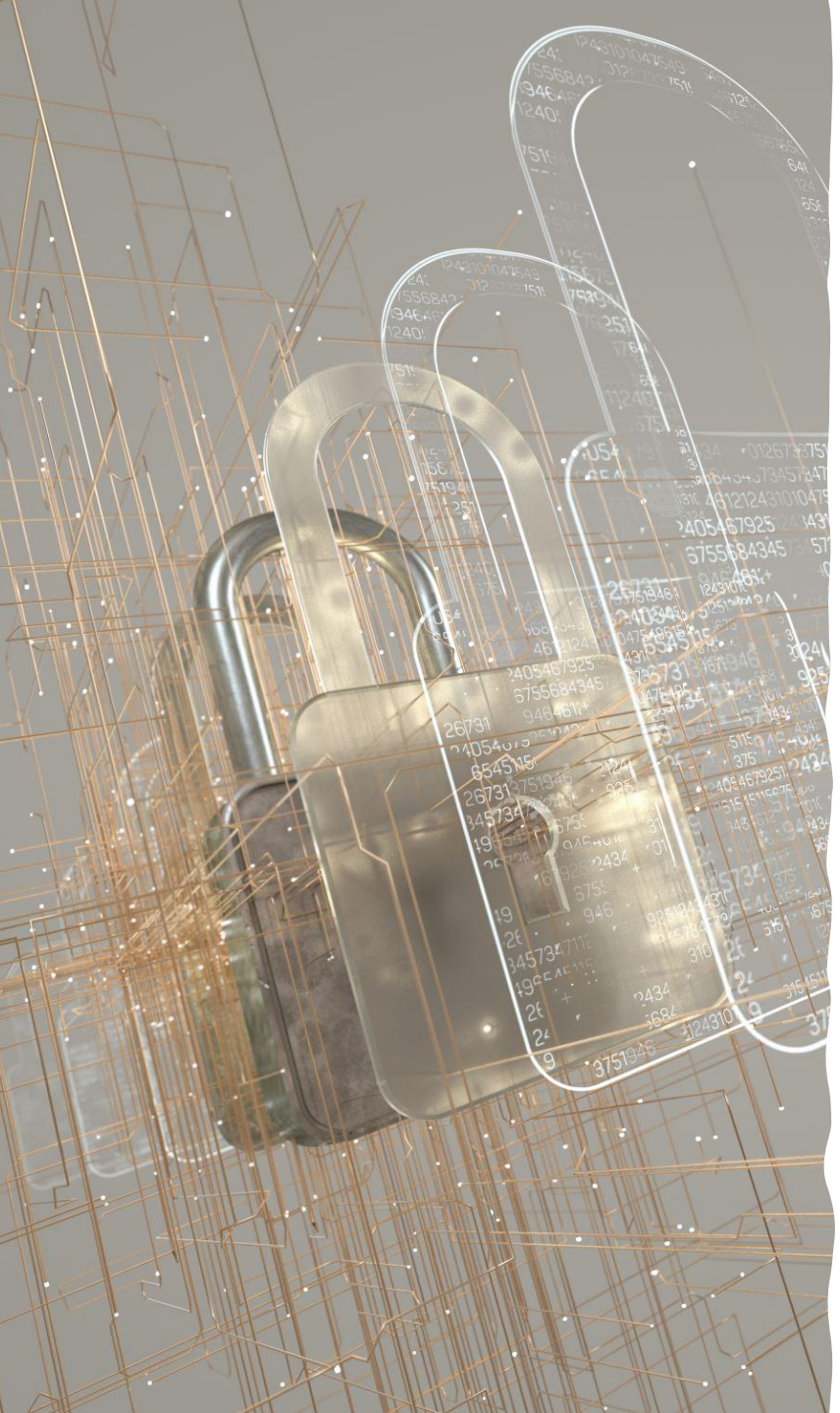


Kerckhoff's Principle

- There is in general no mathematical proof of security for any practical cipher.
- The only way to have assurance that a cipher is secure is to try to break it (legally) (and fail)!
- Kerckhoff's Principle is paramount in modern cryptography:
  - *A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key.*



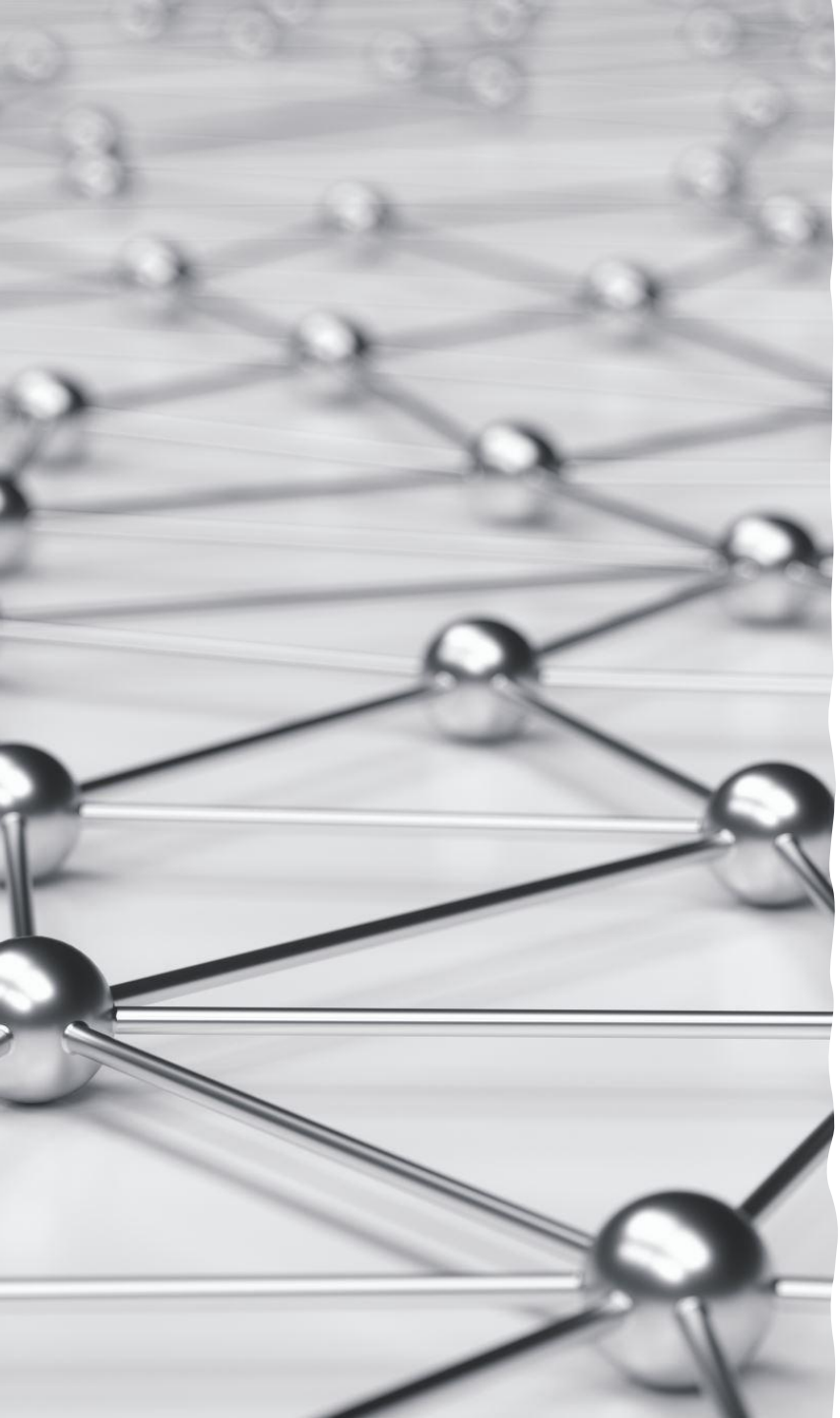
- To achieve Kerckhoff's Principle in practice, we should only use widely-known ciphers that have been cryptanalyzed for several years by good cryptographers!



Services of Cryptosystems

- **Confidentiality:** Renders the information unintelligible except by authorized entities.
- **Integrity:** Data has not been altered in an unauthorized manner since it was created, transmitted, or stored.
- **Authentication:** Verifies the identity of the user or system that created the information.
- **Non-repudiation:** Ensures that the sender cannot deny sending the message.

Can you think of another security service?

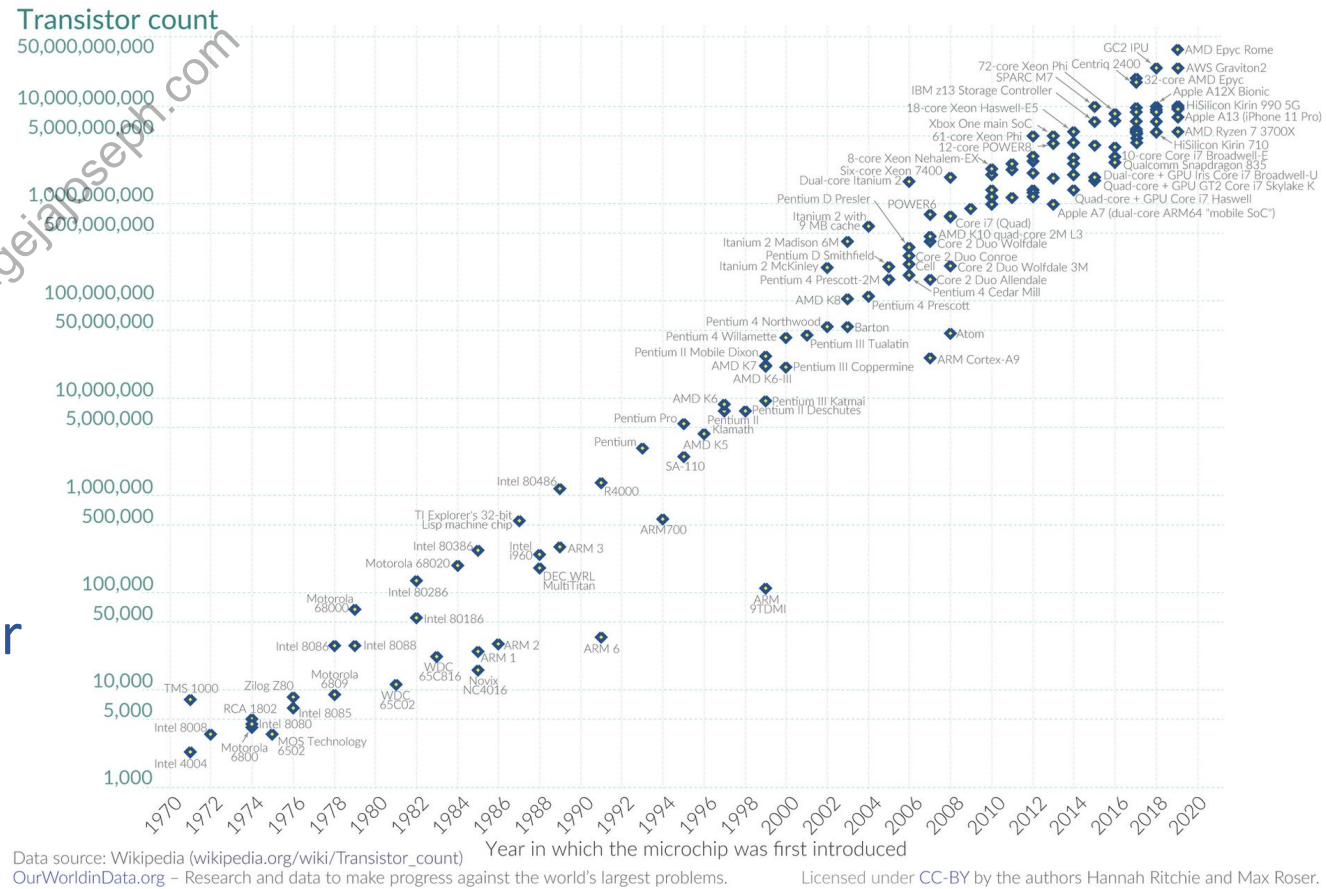


What is Cryptanalysis?

- *Cryptanalysis* is the practice of uncovering flaws within cryptosystems.
- E.g., cryptanalysis has conclusively demonstrated that significant flaws exist in the WEP algorithm.

Brute-Force Attack against Symmetric Ciphers

- Treats the cipher as a black-box
- Attack: $\forall k_i \in K : d_{k_i}(y) \stackrel{?}{=} x$
- Requires (at least) 1 plaintext-ciphertext pair (x, y)
- What key length do we need ?
  - Short-term vs long-term protection
  - Symmetric vs asymmetric crypto
  - Threat and attack model
  - Moore's law
  - etc.
- A long keyspace does not help if other attacks are possible.



Data source: Wikipedia (wikipedia.org/wiki/Transistor_count)
OurWorldinData.org – Research and data to make progress against the world's largest problems.

Black-Box Attack Models

- **Ciphertext-only attack:** An attacker observes ciphertexts without having any knowledge of the corresponding plaintext or the method used to select the plaintext.
- **Known-plaintext attack**: An attacker observes ciphertexts and possesses information about the associated plaintext.
- **Chosen-plaintext attack**: An attacker can request encryption for specific plaintexts of their choice and observe the resulting ciphertexts.
- **Chosen-ciphertext attack**: An attacker can both encrypt and decrypt data.

Affine Cipher

- Extension of the shift cipher; rather than just adding the key to the plaintext, we also multiply by the key

- The key consists of two parts: k = (a, b), which has the restriction: gcd (a, 26) = 1

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_k(x) \equiv (a \,.\, x + b) \bmod 26$
- Decryption: $x = d_k(x) \equiv a^{-1} \,.\, (y - b) \bmod 26$

What is the keyspace of the affine cipher?

- Several attacks are still possible!

Course Overview

- Introduction and Course Overview
- Randomness
- Stream Ciphers
- Block Ciphers (DES, AES)
- Other Aspects of Block Ciphers
- Public-Key Cryptography
- The RSA and Public-Key Cryptosystems
- Digital Signatures
- Hash Functions and MAC
- Key Establishment and Practical Applications
- Course Summary

Practical Components

- Basic programming code will be utilized during most of the lectures.
- Online tools and resources will be employed to identify and address design or implementation weaknesses.
- Theoretical concepts will be applied to real-world industry scenarios, whenever applicable.