**ENC**

**RYPT**

**ION**

VOL 1

METHODS & TECHNIQUES

VOL 1

A cartoon of a person giving thumbs up

Description automatically generated Notes By:

**RABIN ACHARYA**

**Week 1**

**Cryptography**

Cryptography is the science of securing information by transforming it into an unreadable format so only authorized users can access it. Especially, it protects data through encoding (encryption), making it unintelligible to anyone without the decryption key, which reverts it to readable form.

The earliest known use of encryption traces back to Herodotus, the father of history, who documented simple hidden messaging techniques like steganography, where messages were concealed rather than encoded.

In the week 1 discussion the plot of Mary, Queen of Scots is a key example where encryption, espionage (spying) and human error intertwined. She conspired to overthrow her cousin, Queen Elizabeth of England. She with the help of Catholic noblemen used secret messaging using coded letters to plan the assassination of the Elizabeth. However Elizabeth’s secretary Sir Francis Walsingham intercepted Mary’s message and conspiracy was thwarted by Sir Francis, who used cryptography and deception to expose her intentions, leading to her eventual execution.

**Terminologies**

* **Sender and Receiver**

Source/person who wants to send message is sender. The receiver is the one who/whom is the message sent/intended for.

* **Messages, Encryption & Decryption**

A message is plaintext (aka cleartext). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning cipher text back into plaintext is decryption.

Plaintext is denoted by M for message or P for plaintext. It can be a stream of bits, a text, a bitmap, multimedia file or whatever. So, let’s take a look at encryption functions

E(M) = C

In the reverse process, the decryption function D operated on C to produce M:

D( C) = M

Since the whole point of encrypting and then decrypting a message is to recover the original message (plaintext), the following identify must hold true:

D(E(M)) = M

* **Algorithms and Keys**

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. There are two related functions: One for encryption and the other for decryption.

**Applications of Cryptography**

1. **Secure Communication**

Cryptography plays a communication by ensuring only the intended parties can access the content. Messaging apps like WhatsApp use end-to-end encryption, making intercepted messages unreadable to outsiders. This level of security is essential for both personal and professional communication especially in fields like healthcare and finance, where privacy is critical.

1. **Data Integrity and Authentication**

Cryptography maintains data integrity and authenticates sources, ensuring data hasn’t been tampered with. For instance, digital signatures on downloaded files verify their authenticity, alerting users if any modifications occurred. This protection is key in banking, e-commerce, the software, where data trustworthiness is essential.

1. **Secure Storage**

Cryptography secures stored data, making it unreadable to unauthorized users. For example, cloud storage providers encrypt files so that even if a breach occurs, data remains protected. This approach is vital for businesses handling sensitive customer information to prevent data leaks that could lead to financial and reputational harm.

1. **Financial Transaction**

In financial transactions, cryptography secures data in transit, preventing interception or alteration. For instance, SSL/TLS encryption safeguards credit card details during online purchases, protecting customers from fraud. Cryptography’s role in digital payments builds trust, enabling the growth of secure e-commerce.

1. **Authentication and Access Control**

Cryptographic methods support authentication and access control, allowing only authorized access to system. Multi-factor authentication (MFA) combines passwords with device specific codes, providing an additional layer of security. This is widely used to protect sensitive corporate data, adding a strong barrier against breaches.

1. **Blockchain and Cryptocurrency**

Cryptography underpins blockchain and cryptography linking blocks of data in an unalterable chain. Bitcoin, for example, uses cryptographic hashing to secure transaction preventing unauthorized changes. This application extends beyond digital currencies, offering transparent and secure frameworks for various industries like supply chain and voting systems.

**Cryptographic Algorithms**

1. **Shift Cipher (Caesar Cipher)**

Caesar Used this method for the first military purpose during the Gallic Wars.

Creating cipher using 3 characters shift to the right

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F |
| D | E | F | G | H | I |
| G | **H** | **I** | **J** | **K** | **L** |
| J | K | L | M | N | O |
| (It may go on till Z) |  |  |  |  |  |

|  |  |
| --- | --- |
| Encryption examples   * E(BAD) = EDG * E(HIDE) = KLGH | Decryption examples   * D(OLH) = LIE * D(IDGH) = FADE |

1. **Substitution Cypher**

Substitution is the process of using one letter or number to replace and represent another one with a codebook or mathematical model as the encoder and decoder.

Creating substitution model:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F |
| U | K | O | S | 3 | c |
| G | **H** | **I** | **J** | **K** | **L** |
| M | N | 7 | B | W | R |

**(It may go on till Z)**

*We cannot repeatedly use a letter once already used.*

A ~~B~~ ~~C~~ D E F G H I J ~~K~~ L ~~M N~~ ~~O~~ P Q ~~R~~ ~~S~~ T ~~U~~ V ~~W~~ X Y Z

1 2 ~~3~~ 4 5 6 ~~7~~ 8 9

|  |  |
| --- | --- |
| Encryption examples   * E(BAD) = KUS * E(HIDE) = N7S3 | Decryption examples   * D(S7O3) = DICE * D(R7S) = LID |