AI in Encryption

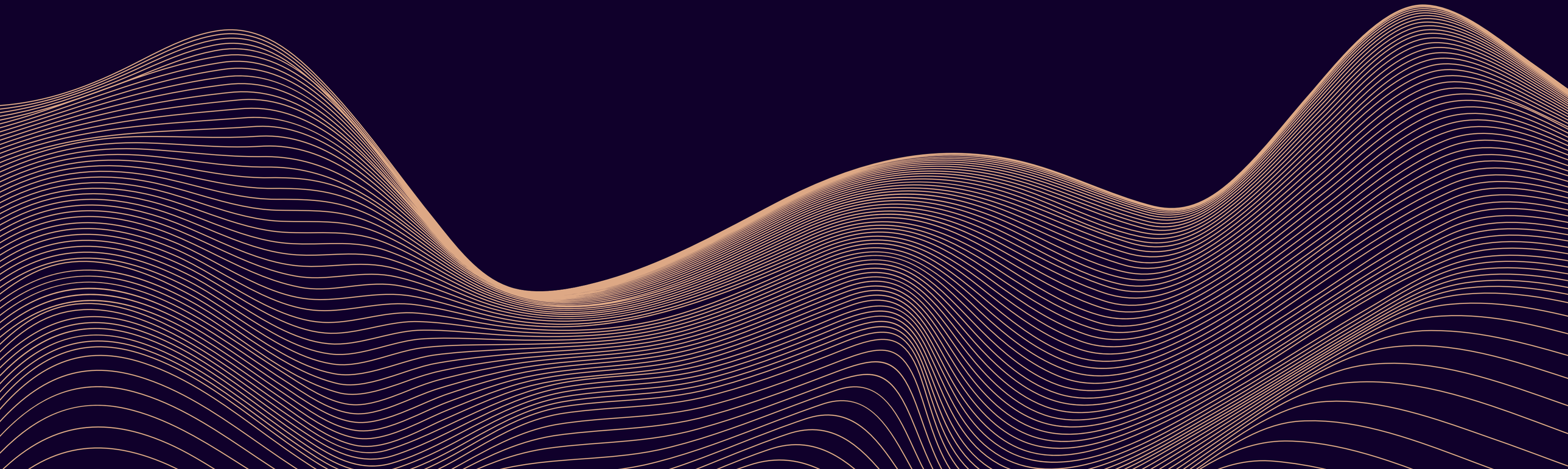
Presentation 1

Vaishnavi D
Aarushi Garg
Ishita Singh
Sunayana

What is Encryption?

- Encryption is a method of converting information or data into a code to prevent unauthorized access.
- It ensures that only those with the correct decryption key can read and understand the original information.
- It is a critical aspect of cybersecurity in today's digital world.

Cipher/ Riddle



There was a death on Treebark Lane. The victim was identified as Mark Oswalt, who recently was married. The police went to the crime scene and they reported the death as a suicide.

Later that day, after the police left, a private detective, hired by the victim's friend who thought it was a murder, searched the crime scene and found a note the police missed.

It read,

"4,3: 8,1:_: 9,1: 2,1: 7,4:_: 6,1:9,3:_: 9,1: 4,3: 3,3: 3,2: !"

The detective took out his cell phone and started dialing the police to tell them about his findings. Once the detective opened the phone to dial, he immediately screamed out, "I SOLVED IT!"

Who was the murderer and how did the detective find out?

Hint

Mark Oswalt used his cell phone for business calls many times a day.

Importance of Data Encryption

Encryption performs four important functions:

- **Confidentiality**: keeps the contents of the data secret
- **Integrity**: verifies the origin of the message or data
- **Authentication**: validates that the content of the message or data has not been altered since it was sent
- **Nonrepudiation**: prevents the sender of the data or message from denying they were the origin

src:https://cloud.google.com/learn/what-is-encryption#importance-of-data-encryption

How encryption works

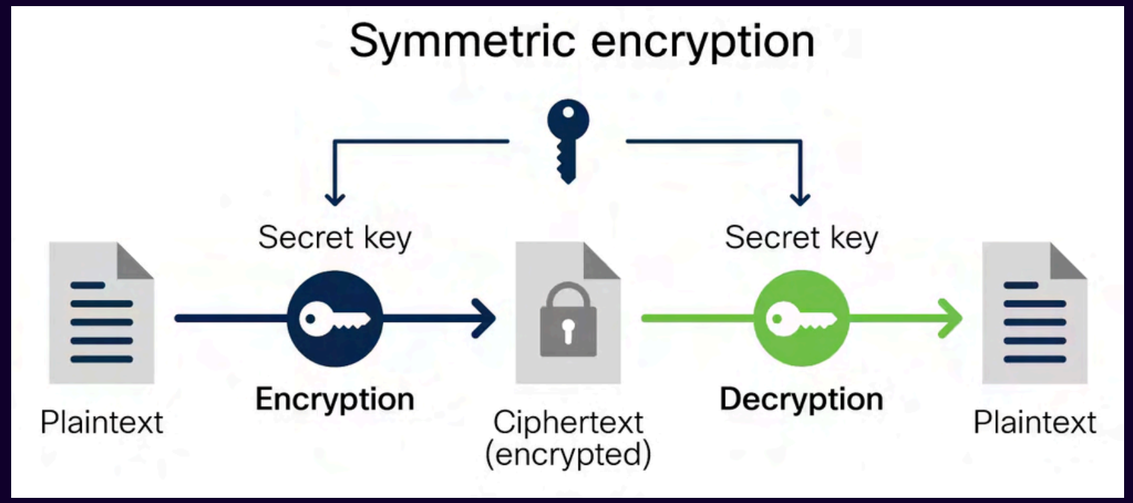
- Encryption works by encoding “plaintext” into “ciphertext,” typically through the use of cryptographic mathematical models known as algorithms.
- One early example of a simple encryption is the “Caesar cipher,” named for Roman emperor Julius Caesar
- Modern cryptography is much more sophisticated, using strings of hundreds (even thousands) of computer-generated characters as decryption keys.

src:https://cloud.google.com/learn/what-is-encryption#importance-of-data-encryption

Types of Encryption Algorithms

1 Symmetric Encryption

It uses the same key for encryption and decryption. Because it uses the same key, symmetric encryption can be more cost effective for the security it provides. That said, it is important to invest more in securely storing data when using symmetric encryption.

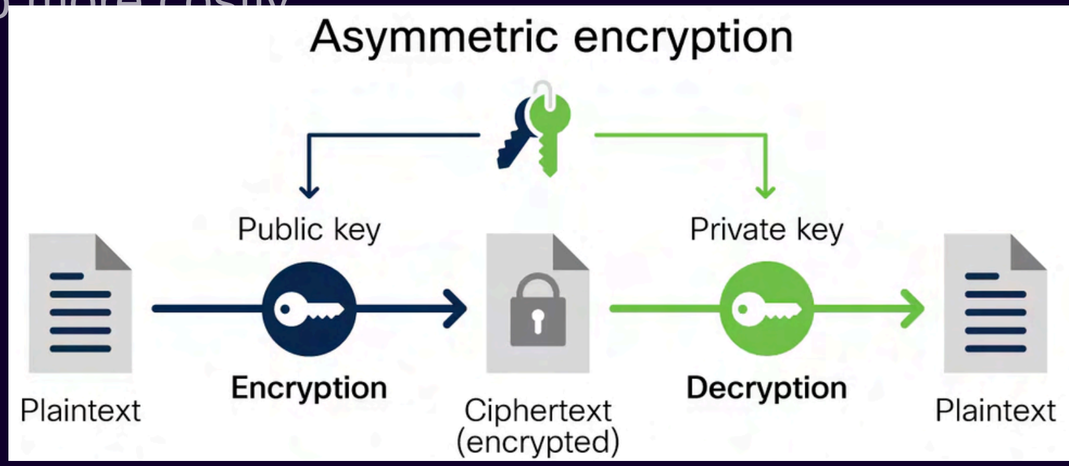


src: https://www.cisco.com/

Types of Encryption Algorithms

2 Asymmetric Encryption

It uses two separate keys: a public key and a private key. Often a public key is used to encrypt the data while a private key is required to decrypt the data. The private key is only given to users with authorized access. As a result, asymmetric encryption can be more effective, but it is also more costly.



src: https://www.cisco.com/

Types of Data Encryption

Triple DES

Triple Data Encryption Standard (3DES) is a symmetric encryption algorithm that encrypts data three times with three 64-bit keys, totaling a 192-bit key length. As a block cipher, it encrypts data in 64-bit segments, but its CBC mode can struggle with high data rates.

RSA

RSA, named after creators Rivest, Shamir, and Adelman, is a standard asymmetric encryption technique using a public and private key. It relies on the difficulty of prime factorization, making it secure but increasingly inefficient at higher security levels.

ECC

Elliptic Curve Cryptography (ECC) uses elliptic curves and number theory to provide robust security with smaller, more efficient keys. For instance, an ECC key of 512 bits offers equivalent security to a 15,360-bit RSA key.

Blowfish

Blowfish, designed by Bruce Schneier in 1993, is a symmetric block cipher with variable-length key encryption ranging from 32 to 448 bits. It is unpatented, unlicensed, and freely available for public use.

AES

Due to increased brute-force attacks on DES, the Advanced Encryption Standard (AES), originally named Rijndael, was introduced in 2002. AES, a symmetric block cipher with 128, 192, and 256-bit keys, is used to protect classified government information and sensitive data.

What does AI do

- At its core, AI-powered encryption utilizes machine learning algorithms to analyze and adapt to new cyber threats continuously, making it an incredibly dynamic and proactive defense mechanism.
- By employing AI-driven pattern recognition and predictive analytics, this encryption method can rapidly identify potential vulnerabilities and create tailored encryption protocols to thwart would-be attackers.

Source:- https://www.sciencedirect.com/science/article/abs/pii/S0925231215006785
https://datafloq.com/read/ai-powered-encryption-a-new-era-in-cybersecurity/#:~:text=Moreover%2C%20the%20integration%20of%20AI,unauthorized%20access%20or%20data%20breaches.

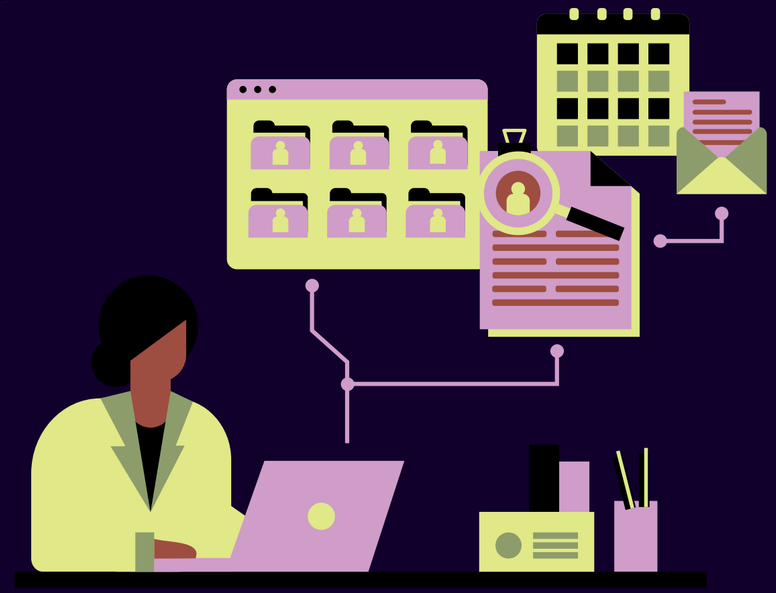
RESOURCES

src:https://cloud.google.com/learn/what-is-encryption#importance-of-data-encryption

src:https://cloud.google.com/learn/what-is-encryption#importance-of-data-encryption

src: https://www.cisco.com/

https://www.sciencedirect.com/science/article/abs/pii/S0925231215006785
https://datafloq.com/read/ai-powered-encryption-a-new-era-in-cybersecurity/#:~:text=Moreover%2C%20the%20integration%20of%20AI,unauthorized%20access%20or%20data%20breaches.




Thank
You