DSN4095 - Capstone Project Phase - 2 Review - 1

CRYPTOGRAPHY AND INFORMATION THEORY

By: Group-100

Supervised by: Dr.Mohammad Sultan Alam

Group Members:

Abhishek Kumar	21BCE10084
Karan Kumar Chauhan	21BCE10243
Radadiya Deep Rameshbhai	21BCE11343
Vikash Kumar Sinha	21BCE11500
Amul Gupta	21BCE11606

Contents:

INTRODUCTION

- Entropy and Key Generation
- Symmetric Algorithm Performance
- Asymmetric Algorithm Efficiency

01 02 03

Entropy and Key Generation: The study analyzes key generation and entropy for both symmetric and asymmetric cryptographic algorithms, using Shannon entropy to quantify randomness and security.

Symmetric Algorithm Performance: Among symmetric algorithms (AES, 3DES, DES, Blowfish), AES demonstrated the highest entropy with its 256-bit key size, while DES, with its outdated 64-bit key, showed the lowest entropy, highlighting its obsolescence.

Asymmetric Algorithm Efficiency: Asymmetric algorithms (RSA, DSA, ECC) have lower entropy per byte but rely on larger key sizes for security. ECC is particularly notable for achieving strong security with smaller keys compared to RSA and DSA.

BRIEF INTRODUCTION ON INFORMATION THEORY

- INFORMATION THEORY IS A BRANCH OF APPLIED MATHEMATICS AND ELECTRICAL ENGINEERING THAT DEALS WITH THE QUANTIFICATION, STORAGE, AND COMMUNICATION OF INFORMATION. IT WAS FOUNDED BY CLAUDE SHANNON IN HIS LANDMARK 1948 PAPER "A MATHEMATICAL THEORY OF COMMUNICATION." THE PRIMARY GOALS OF INFORMATION THEORY ARE TO UNDERSTAND THE LIMITS AND EFFICIENCY OF DATA COMPRESSION AND TRANSMISSION OVER COMMUNICATION CHANNELS.

KEY CONCEPTS IN INFORMATION THEORY INCLUDE:

- INFORMATION ENTROPY: ENTROPY QUANTIFIES THE AMOUNT OF UNCERTAINTY OR RANDOMNESS IN A SET OF DATA.

- SHANNON'S THEOREMS: NOISELESS CODING THEOREM (SHANNON'S FIRST THEOREM): THIS THEOREM STATES THAT THE ENTROPY OF A SOURCE GIVES THE THEORETICAL LIMIT OF HOW MUCH A SOURCE CAN BE COMPRESSED WITHOUT LOSING INFORMATION.

- CHANNEL CAPACITY: THIS IS THE MAXIMUM RATE AT WHICH INFORMATION CAN BE RELIABLY TRANSMITTED OVER A COMMUNICATION CHANNEL.

BRIEF INTRODUCTION ON INFORMATION THEORY IN CRYPTOGRAPHY

Self Information Theory

Self-Information (Shannon Information Content) states that

- A discrete random variable, can take on different values, each with an associated probability.
- In simpler terms, it tells us how surprising or informative it is to find out that the box contains the value.

The Formula for Information Theory is:-

$$I(x_i) = -\log\left(P_X(x_i)\right)$$

BRIEF INTRODUCTION ON INFORMATION THEORY IN CRYPTOGRAPHY

Now, if the events represented by X and Y are independent, the joint probability of both events occurring together can be calculated as the product of their individual probabilities:

$$P_{(X,Y)}(x_i, y_j) = P_X(x_i).P_Y(y_j)$$

Using this relationship, we can rewrite the self-information for the pair:

$$I(x_i, y_j) = -\log(P_X(x_i).P_Y(y_j))$$

BRIEF INTRODUCTION ON INFORMATION THEORY IN CRYPTOGRAPHY

ENTROPY

Entropy measures the uncertainty or randomness in a system or message, with higher unpredictability leading to higher entropy. In cryptography, Claude Shannon introduced the idea of perfect secrecy, where ciphertext reveals no information about the plaintext, and understanding entropy is key to evaluating encryption security.

The entropy, denoted as H(X), can be mathematically expressed as:

$$H(X) = E(I[(x_i)] = \sum I(x_i) \mathrm{P}_X(x_i)$$

Substituting the definition of self-information, we have:

$$H(X) = \sum_{\mathrm{i}} \mathrm{P}_X(\mathrm{x_i}) \log\left(\frac{1}{P_X(\mathrm{x_i})}\right)$$

$$= -\sum_{\mathrm{i}} \mathrm{P}_X(\mathrm{x_i}) \log \mathrm{P}_X(\mathrm{x_i})$$

MUTUAL INFORMATION

Mutual information measures how much two variables share information,quantifying how much knowing one reveals about the other.

To find this capacity, we maximize the average mutual information I(X;Y) over all possible distributions of the input X:

$$C = \max_{P(X)} I(X;Y)$$

where c = channel capacity

BRIEF INTRODUCTION ON INFORMATION THEORY IN CRYPTOGRAPHY

ERROR CORRECTION AND DETECTION

Error detection identifies errors in transmitted data, commonly using Cyclic Redundancy Check (CRC). Similarily, In case of Error correction, it not only detects errors but also corrects them, ensuring that the received data matches the original transmission using Error-Correcting Codes (ECC).

Given a data sequence represented as a polynomial D(x) and a generator polynomial G(x), the CRC is calculated as follows:

$$R(x) = D(x) \times x^n \bmod G(x)$$

Here, n is the degree of the generator polynomial G(x), and R(x) is the remainder, which serves as the CRC code.
The transmitted message is then:

$$T(x) = D(x).x^n + R(x)$$

CRYPTOGRAPHY WITH INFORMATION THEORY

- Information theory enhances cryptography by providing security that doesn’t rely on solving complex math problems, instead using physical factors like noise for unconditional security.

- Key applications include unconditionally secure secrecy, authentication, and key agreement, which can be achieved using these principles.

01 02 03

- Important cryptographic tools like perfect secrecy, secret sharing, wire-tap channels, and broadcast channels are introduced, showing their role in improving cryptographic systems.

INFORMATION-THEORETIC SECURITY IN CRYPTOGRAPHY

- Information-theoretic security represents a major shift from traditional cryptography, which relies on the assumption that certain problems are hard to solve within a reasonable time.

- Unlike computational security, it ensures that a system remains secure even against adversaries with unlimited computing power. This concept is based on Claude Shannon's foundational work in information theory.

INFORMATION-THEORETIC SECURITY IN CRYPTOGRAPHY

- **Perfect Secrecy:** A ciphertext is perfect when the original message (X), the ciphertext (Y), and a public random value (R) are completely independent of each other. This means no information about the message can be learned from the ciphertext. This idea comes from Shannon's theorem.

- **Secret Sharing:** Information theory is now used to find limits on how much information each participant gets in perfect secret sharing. In this method, a secret is split among participants so that only certain groups can recover it, while others get no information about the secret.

01 02 03

INFORMATION-THEORETIC SECURITY IN CRYPTOGRAPHY

- **Wire-tap channel:** Wyner introduced the wire-tap channel model in 1975, where an eavesdropper (Eve) listens to a message between Alice and Bob through a noisy channel. Eve's chances of correctly guessing the message decrease as Alice adds random bits to her transmission. Bob, who gets the message without errors, can easily decode it, but Eve's guess becomes less accurate.

- **Broadcast channel:** Csiszár and Körner extended Wyner's model to a more general communication channel, where Eve’s message isn’t necessarily worse than Bob’s. The system depends on the probability of what both Bob and Eve receive, based on the message Alice sends.

01 02 03

Encryption and Decryption Models

- **Symmetric Encryption -** Symmetric encryption is a method where the same key is used for both encryption and decryption. This means that the sender and the receiver must both have access to the same secret key to encrypt and decrypt the data. The process is relatively fast and straightforward, making it suitable for encrypting large amounts of data.

- **AES (Advanced Encryption Standard) -** It is widely used for securing sensitive data. AES operates on fixed block sizes of 128 bits and supports key sizes of 128, 192, or 256 bits. The encryption process involves multiple rounds of transformation based on the key

- **Blowfish:** A symmetric-key block cipher which operates on 64-bit blocks of data, making it suitable for encrypting relatively small chunks of information.

- **3DES (Triple Data Encryption Standard) -** 3DES is a symmetric-key block cipher used in cryptography to provide secure data encryption. It is an enhancement of the original DES (Data Encryption Standard) algorithm. 3DES applies the DES algorithm three times to each data block, hence the name "Triple DES." The goal is to increase the security of DES, which was considered vulnerable due to its relatively short key length.

- **DES (Data Encryption Standard) -** DES operates on 64-bit blocks of plaintext and uses a 56-bit key (after dropping 8 parity bits from the original 64-bit key) to encrypt and decrypt data.DES employs a series of complex transformations, including permutations and substitutions, over multiple rounds (16 rounds in total) to achieve security. Each round uses a different subkey derived from the main key. DES is now considered insecure for many applications due to its relatively short key length, which makes it vulnerable to brute-force attacks.

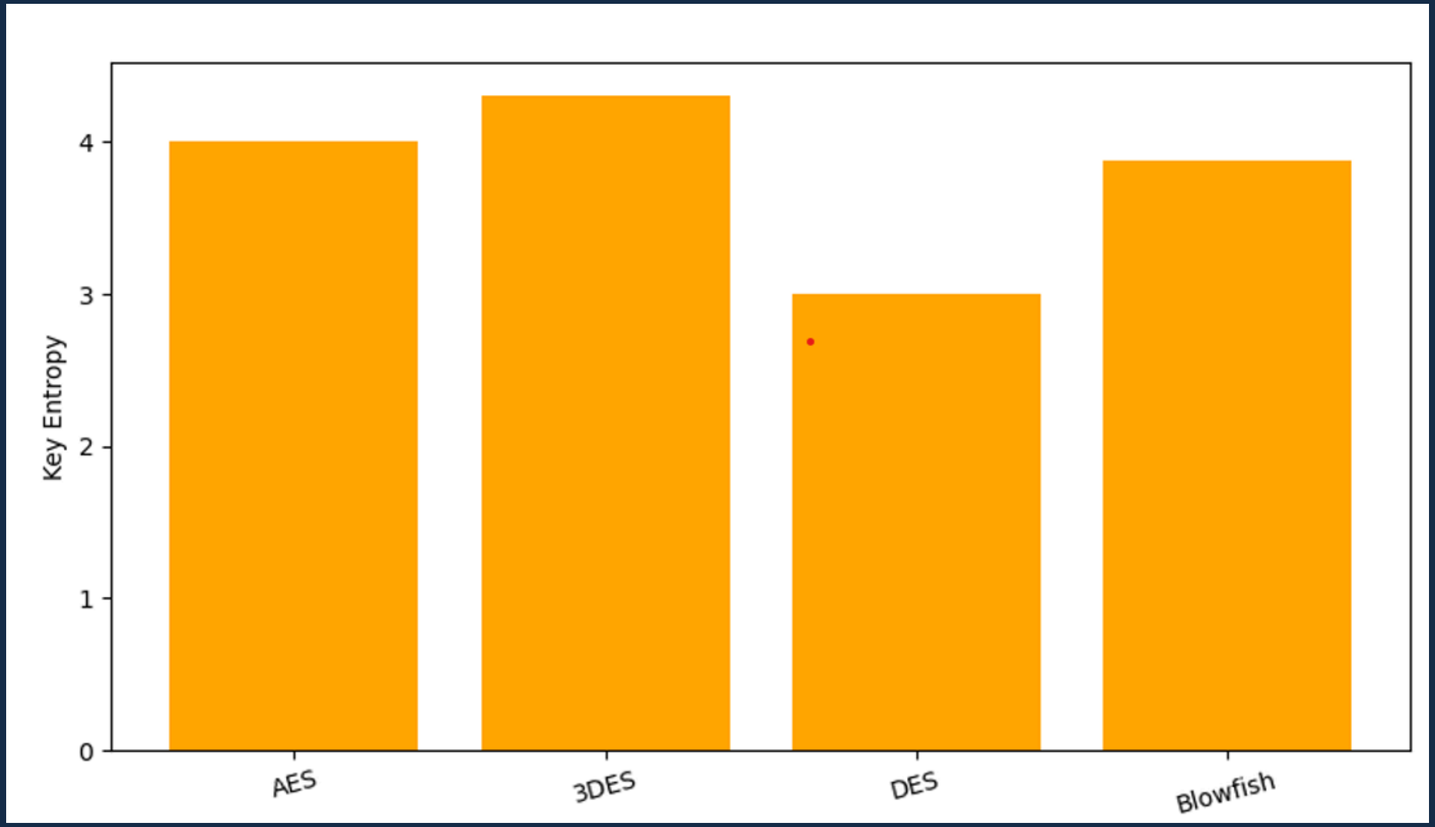
- **<u>Asymmetric Encryption</u> -** Asymmetric encryption, also known as public-key cryptography, uses two different keys: one for encryption (public key) and another for decryption (private key). The public key is shared openly, while the private key is kept secret by the owner. This method allows secure communication even if the public key is shared openly because only the corresponding private key can decrypt the message.

- **RSA (Rivest-Shamir-Adleman) -** RSA is a public-key cryptosystem used for secure data transmission. It is one of the first practical cryptosystems and is widely used for secure communication, especially for encrypting sensitive data and authenticating digital signatures. The security of RSA comes from the difficulty of factoring large composite numbers, specifically the product of two large prime numbers.

- **DSA (Digital Signature Algorithm) -** In Cryptography, DSA is used to generate a digital signature by encrypting a message hash with a private key, which can be verified using the corresponding public key. The integrity of the message is ensured because the signature is tied to both the message and the key.

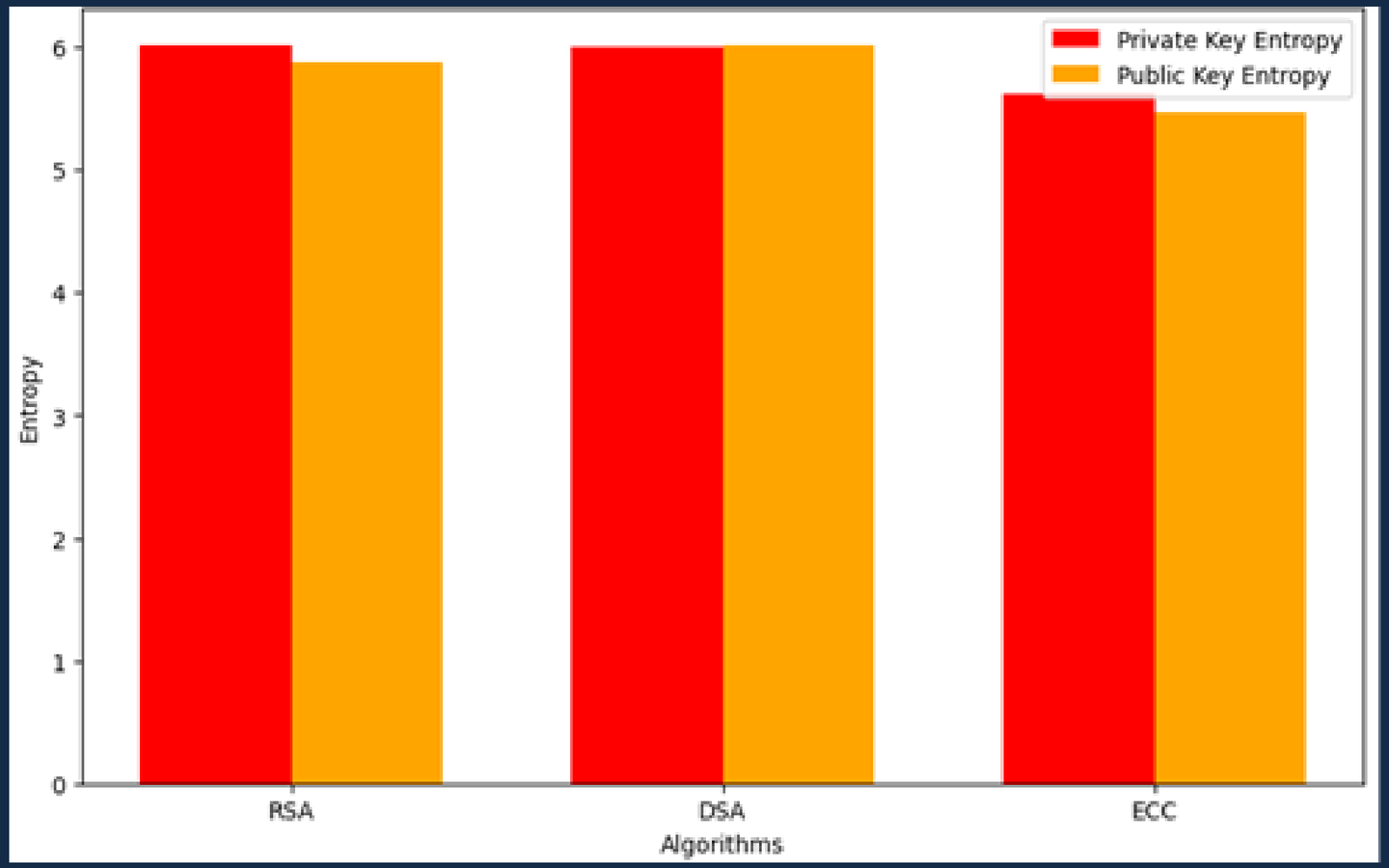
- **ECC (Elliptic Curve Cryptography) -** ECC is based on the algebraic structure of elliptic curves over finite fields. The underlying mathematical problem that ECC leverages is the difficulty of the Elliptic Curve Discrete Logarithm Problem , which is computationally infeasible to solve with current technologies for large key sizes. In ECC, security is achieved by generating keys from points on an elliptic curve. Given two points on the curve, their sum is also a point on the curve, and scalar multiplication of a point forms the basis for cryptographic operations.

Conclusion



In this comparison, the key entropy was calculated for different symmetric algorithms to understand their randomness and security levels. 3DES exhibited the highest key entropy, followed closely by AES and Blowfish. DES, being an older encryption standard, demonstrated the lowest entropy, confirming its reduced security in modern contexts. These findings reinforce the use of AES and Blowfish in current encryption standards, whereas DES has been largely deprecated

Conclusion



·RSA and DSA have nearly identical entropy values for private and public keys, which reflects their reliance on large key sizes and complex mathematical operations.

·ECC, while having slightly lower entropy, provides a more efficient solution with smaller key sizes without compromising much on security.

·In general, higher entropy correlates with more robust cryptographic strength, and all three algorithms perform well, with slight trade-offs between key size and efficiency.

THANK YOU