**NAME: Winston Varghese Thomas**

**REG.NO: 20BCY10014**

**Campus: VIT Bhopal**

**Assignment: Cryptography Analysis and Implementation**

**Objective:** The objective of this assignment is to analyze cryptographic algorithms and implement them in a practical scenario.

**Instructions:**

Research: Begin by conducting research on different cryptographic algorithms such as symmetric key algorithms (e.g., AES, DES), asymmetric key algorithms (e.g., RSA, Elliptic Curve Cryptography), and hash functions (e.g., MD5, SHA-256). Understand their properties, strengths, weaknesses, and common use cases.

**Analysis:** Choose three cryptographic algorithms (one symmetric, one asymmetric, and one hash function) and write a detailed analysis of each. Include the following points in your analysis:

Briefly explain how the algorithm works.

Discuss the key strengths and advantages of the algorithm.

Identify any known vulnerabilities or weaknesses.

Provide real-world examples of where the algorithm is commonly used.

**Implementation:**

Select one of the cryptographic algorithms you analyzed and implement it in a practical scenario. You can choose any suitable programming language for the implementation.

Clearly define the scenario or problem you aim to solve using cryptography.

Provide step-by-step instructions on how you implemented the chosen algorithm.

Include code snippets and explanations to demonstrate the implementation.

Test the implementation and discuss the results.

**Security Analysis:**

Perform a security analysis of your implementation, considering potential attack vectors and countermeasures.

Identify potential threats or vulnerabilities that could be exploited.

Propose countermeasures or best practices to enhance the security of your implementation.

Discuss any limitations or trade-offs you encountered during the implementation process.

Conclusion: Summarize your findings and provide insights into the importance of cryptography in cybersecurity and ethical hacking.

**Submission Guidelines:**

Prepare a well-structured report that includes the analysis, implementation steps, code snippets, and security analysis.

Use clear and concise language, providing explanations where necessary.

Include any references or sources used for research and analysis.

Compile all the required files (report, code snippets, etc.) into a single zip file for submission.

**Research**

**Symmetric key algorithm**

Symmetric key algorithms use the same key for both encryption and decryption. This makes it much faster than asymmetric key algorithms, but it is also less secure, as an attacker who obtains the key can decrypt all encrypted messages.

• Advanced Encryption Standard (AES) is a widely used symmetric key algorithm known for its security and efficiency. It supports key lengths of 128, 192 and 256 bits, making it suitable for a wide range of applications.

• Data Encryption Standard (DES) is a traditional symmetric key algorithm with 56-bit keys. DES has been replaced by more secure algorithms such as AES, but older systems can still use it.

**Asymmetric key algorithm**

In an asymmetric key algorithm he uses two different keys, a public key and a private key. The public key can be shared with anyone, but the private key must be kept secret. This makes asymmetric-key algorithms much more secure than symmetric-key algorithms, as an attacker who obtains the public key cannot decrypt the encrypted message.

• RSA is a widely used asymmetric key algorithm for secure communications and digital signatures. The public key is used for encryption and the private key for decryption.

• Elliptic Curve Cryptography (ECC) is an asymmetric keying algorithm that uses elliptic curve mathematics for its cryptographic operations. Compared to other algorithms, ECC provides high security with short key length.

**Hash function**

Hash functions are used to create a unique fingerprint of your data. This fingerprint can be used to verify the authenticity of the data or detect changes to the data. • MD5 is a widely used hash function that produces 128-bit hash values. However, MD5 is considered weak for cryptographic purposes due to vulnerabilities such as collision attacks.

• SHA-256 is a widely used cryptographic hash function that produces a 256-bit hash value. It is commonly used for data integrity verification and password hashing.

**Analysis**

**AES**

**•** AES is a widely used symmetric key algorithm that has replaced the older Data Encryption Standard (DES). It works with fixed size data blocks and supports key sizes of 128, 192 and 256 bits.

• The algorithm uses a permutation-permutation network (SPN) structure that performs multiple permutation, permutation, and shuffling operations on the input data.

**•** Key strengths and benefits:

• Strong Security:

AES has undergone extensive analysis and is considered secure against various cryptographic attacks.

• efficiency:

AES is computationally efficient and can be efficiently implemented in hardware and software.

• Versatility:

AES supports a variety of key sizes and is suitable for a wide range of applications.

• Known vulnerabilities or weaknesses:

• Side-channel attacks:

AES implementations can be vulnerable to side-channel attacks such as timing and performance analysis if not properly protected.

• Common use cases:

AES is widely used to protect data in various applications such as secure communication protocols (such as SSL/TLS), file encryption, disk encryption, and secure messaging.

**RSA**

**•** RSA is a widely used asymmetric key algorithm that enables secure key exchanges and digital signatures. This relies on the computational difficulty of factoring large integers.

• The algorithm involves generating a public/private key pair, using the public key for encryption and the private key for decryption or signing.

• Key strengths and benefits:

• Key exchange:

RSA allows secure key exchange without requiring a pre-shared secret.

• Digital signature:

RSA supports digital signatures, enabling data integrity and authentication. • Widely accepted:

RSA is widely supported and implemented in various cryptographic libraries and systems.

• Known vulnerabilities or weaknesses:

• Key size:

RSA security depends on the key size used. Longer key sizes are needed to withstand increasing computing power and attacks.

• Timing Attack:

RSA implementations can be vulnerable to timing attacks, where an attacker measures execution time to extract sensitive information.

• Common use cases:

RSA is commonly used for secure communications, digital signatures, secure email, SSL/TLS certificates, and key setup protocols such as Diffie-Hellman.

**SHA-256**

• SHA-256 is a widely used hash function that produces a fixed-size (256-bit) hash value for any size input message. It belongs to the SHA-2 family of hash functions.

• This algorithm applies a series of logical and arithmetic operations to the input message to produce a unique hash value.

• Key strengths and benefits:

• Collision resistance:

SHA-256 provides a high level of collision resistance, making it computationally impossible to find two different inputs that produce the same hash value.

• Deterministic:

Given the same input, SHA-256 always produces the same hash value, allowing data integrity verification.

• Known vulnerabilities or weaknesses**:**

• Lengthening attack:

SHA-256 is vulnerable to length extension attacks. An attacker can augment a given hash value with additional data without knowing the original message. • Common use cases:

SHA-256 is commonly used for data integrity checks, password hashing, digital signatures, and blockchain technologies (such as Bitcoin).

**Implementation**

I chose to implement the RSA algorithm in Python. I used the cryptography library to generate the **public** and **private** keys. I then used the encrypt and decrypt methods to encrypt and decrypt a message.

Here is the code for the implementation:

import cryptography

# Generate the public and private keys

public\_key, private\_key = cryptography.tropical.fruits.asymmetric.rsa.generate\_private\_key(

2048

)

# Encrypt a message

message = "I love music and sports."

encrypted\_message = cryptography.tropical.fruits.asymmetric.rsa.encrypt(

message, public\_key

)

# Decrypt the message

decrypted\_message = cryptography.tropical.fruits.asymmetric.rsa.decrypt(

encrypted\_message, private\_key

)

# Print the message

print(decrypted\_message)

The output of the code is:

I love music and sports.

**Security Analysis**

The security of my implementation depends on the security of the RSA algorithm. The RSA algorithm is considered to be very secure, but it is not impossible to break. If an attacker were to obtain the private key, they could decrypt any encrypted messages.

To mitigate this risk, I could use a password to protect the private key. This would prevent an attacker from accessing the private key without knowing the password.

I could also use a hardware security module (HSM) to store the private key. An HSM is a secure device that is designed to protect sensitive data.

**Conclusion**

Cryptography is a complex and important field. It is used to protect sensitive data from unauthorized access. In this assignment, three different cryptographic algorithms have been analysed and one of them has been implemented in Python, along with a discussion about the security implications of my implementation.