Applied Cryptography

Student Full Name
National College of Ireland
Course Full Title
Instructor Full Name
13-01-2023, 23:55

Applied Cryptography

Question 1: Character Count Calculation Method for Plaintext Generation

The student number is X22196030

1. Extracting the middle two digits:

A = 6, B = 0

2. Calculate the sum:

Sum = A + B = 6 + 0 = 6

3. Choose a random number between 10 and 40:

Let's say R = 13

4. Add R and Sum:

N = R + Sum = 13 + 6 = 19

5. Generating a random plaintext with 19 characters:

1C2G3KmoQSZXvTRPnLjH

Question 2: Comprehensive Security Policy: Integrating Key Principles for Data Protection

Dublin Financial Institute Comprehensive Data Protection

1. Problem Statement:

Dublin Financial Institute faces a critical challenge in safeguarding sensitive data from the growing cybersecurity threats in today's landscape. The absence of a comprehensive security policy exposes the institution to potential financial losses, reputational damage, and legal ramifications resulting from data breaches. To fortify the organization against cyber threats and mitigate associated risks, a robust encryption policy is urgently needed. This policy aims to ensure the confidentiality, integrity, non-repudiation, and authenticity of sensitive information, thereby safeguarding the institution's assets and maintaining the trust of its stakeholders.

2. Solution: Encryption Policy

2.1. Overview:

The proposed encryption policy will serve as a foundational element in Dublin Financial Institute's cybersecurity strategy. It encompasses a multi-faceted approach, incorporating cutting-edge encryption techniques to protect sensitive data across various aspects of the organization's operations.

2.2. Implementation Scope:

This encryption policy will be implemented across all facets of Dublin Financial Institute's operations, covering data creation, storage, transmission, and modification. It will encompass databases, communication channels, file systems, and any medium where sensitive information resides.

2.3. Intended Audience:

- All Dublin Financial Institute's employees.
- Everything one accessing or handling Dublin Financial Institute's data.

2.4. Approach:

a. Confidentiality:

- Encryption Algorithm (AES): The proposed encryption policy will employ the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode to guarantee the confidentiality of sensitive data.
- Process:

1. Generation of a session-specific symmetric key.
2. Implementation of AES in CBC mode for encryption.
3. Encryption of the provided plaintext "1C2G3KmoQSZXvTRPnLjH" using AES.

b. Integrity:

- Hash Function (SHA-256): The encryption policy will apply the SHA-256 cryptographic hash function to verify data integrity.

- Process:

1. Computation of the hash of the plaintext before encryption.
2. Sending the hash alongside the encrypted data.
3. Recalculation and comparison of the hash at the receiving end.

c. Non-repudiation:

- Digital Signatures: The encryption policy will implement digital signatures to ensure non-repudiation.
- Process:

1. Signing both the plaintext and the hash with digital signatures.
2. Verifying the signatures at the recipient's end.

d. Authenticity:

- Public Key Infrastructure (PKI): The policy will utilize a Public Key Infrastructure for the issuance and verification of digital certificates, ensuring the authenticity of communicating parties.
- Process:

1. Implementation of PKI for digital certificate management.
2. Utilization of digital certificates for authenticating communicating parties.

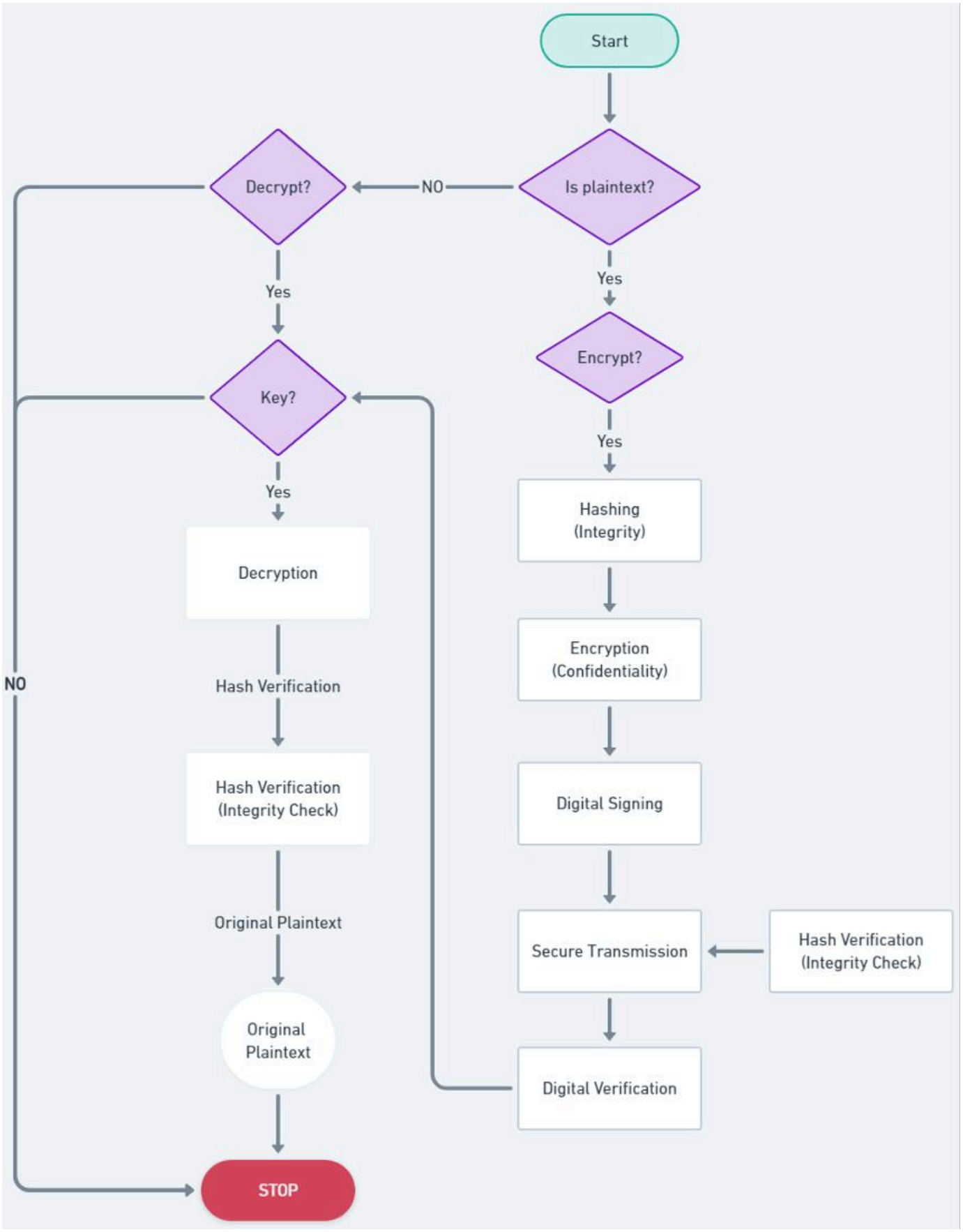

Figure 1. A visual representation of the end-to-end process, showcasing each step in the security framework

2.5. Disadvantages:

Despite the robust security measures, the proposed encryption policy introduces certain challenges that must be considered.

a) Computational Overhead:

- Description: The encryption and hashing processes may introduce computational overhead, impacting system performance.
- Impact: Medium
- Mitigation: Optimization of algorithms, utilization of hardware acceleration, and implementation of efficient key management practices.

b) Key Management Complexity:

- Description: Managing encryption keys, digital signatures, and certificates can become complex, especially at scale.
- Impact: High
- Mitigation: Implementation of a robust key management system, automation of key rotation, and utilization of key management protocols.\

c. Dependency on Trust in Certificate Authorities (CAs):

- Description: Authenticity relies on trust in CAs. Compromised or untrustworthy CAs can undermine the entire security framework.
- Impact: Critical
- Mitigation: Regular audit and validation of CAs, implementation of certificate pinning, and diversification of trust anchors.

By implementing this comprehensive encryption policy, Dublin Financial Institute aims to enhance its data security measures while acknowledging and proactively mitigating the associated disadvantages.

Question 3: Secure Data Transmission: Applying Multi-Method Encryption Scheme with Justified Security Principles

*A*pplication of Security Principles to Chosen Plaintext:

1. *Confidentiality:*

Vigenère Cipher: Finance to Management

- Key Generation: Finance will generate a secret key, e.g., "FINANCEKEY."
- Encryption Process: Each character of the plaintext will be shifted based on the corresponding character in the key.
- Justification: Vigenère Cipher will transform the plaintext in a key-dependent manner, ensuring confidentiality.
- Calculation Example:
- Plaintext: 1C2G3KmoQSZXvTRPnLjH,
- Key: FINANCEKEYFINANCEKEYF,
- Ciphertext: BZ3R4IlbWLIHoVUGXnD

2. Integrity:

Pseudo One-Time Pad: Management to Finance

- Keystream Generation: Management will generate a pseudorandom keystream, e.g., "01010101010101010101010101."
- Encryption Process: XOR operation of the plaintext with the keystream will ensure data integrity.
- Justification: Pseudo One-Time Pad will provide high integrity by XORing the plaintext with a truly random keystream.
- Calculation Example:

Plaintext: 1C2G3KmoQSZXvTRPnLjH,

Keystream: 01010101010101010101010101,

Ciphertext: 1D2F3JnpRTYUcVSQmOe

3. *Non-repudiation:*

RSA Public Key Cryptography: Finance to Management

- Key Pair Generation: Finance will generate a public-private key pair.
- Digital Signature: Hashing the plaintext and encrypting the hash with the private key will create a digital signature. The plaintext will then be encrypted with the recipient's public key.
- Justification: RSA will provide non-repudiation by associating a digital signature with the sender's private key.
- Calculation Example:
- Plaintext: 1C2G3KmoQSZXvTRPnLjH,

Hash: SHA256(1C2G3KmoQSZXvTRPnLjH),

Digital Signature: Sign (Hash) with Private Key,

Encrypted Plaintext: Encrypt (Plaintext) with Recipient's Public Key

3. Authenticity:

RSA Public Key Cryptography: Management to Finance

- Key Pair Generation: Management will generate a public-private key pair.
- Digital Signature: Hashing the plaintext and encrypting the hash with the private key will create a digital signature. The plaintext will then be encrypted with the recipient's public key.
- Justification: RSA will ensure authenticity by associating a digital signature with the sender's private key.
- Calculation Example:

Plaintext: 1C2G3KmoQSZXvTRPnLjH,

Hash: SHA256(1C2G3KmoQSZXvTRPnLjH),

Digital Signature: Sign (Hash) with Private Key,

Encrypted Plaintext: Encrypt (Plaintext) with Recipient's Public Key

Question 4: Understanding Diffie-Hellman Key Exchange and Limitations of Symmetric Key Cryptography in Internet Communications

1. **Diffie-Hellman Key Exchange Protocol: Securing Key Exchange in Public Networks:**

The Diffie-Hellman key exchange protocol is considered a cornerstone in modern cryptography, specifically designed to address the challenge of secure key exchange over public networks. Its ingenious concept enables two parties to generate a shared secret key over an insecure communication channel without exchanging any private information. This essay explores how the Diffie-Hellman protocol tackles the issue of secure key exchange and breaks down its main operational steps.

Addressing the Challenge:

Secure key exchange is a critical aspect of cryptographic systems, particularly in public networks where eavesdropping and interception pose significant threats. Traditional key exchange methods involve transmitting secret keys directly, making them susceptible to interception. Diffie-Hellman introduces a novel approach, relying on mathematical properties rather than secure channels.

The protocol's strength lies in the difficulty of solving the discrete logarithm problem, which forms the basis of its security. Even if an eavesdropper intercepts the exchanged values, computing the shared secret key without knowledge of the private keys is computationally infeasible.

Main Steps of Diffie-Hellman:

a. Key Generation:

- Each party independently generates a public-private key pair.
- The public key is shared openly, while the private key remains confidential.

b. Exchange Public Keys:

- Parties exchange their public keys openly but do not share their private keys.
- The openness of this exchange is crucial for the protocol's success.

c. Shared Secret Calculation:

- Each party combines its private key with the received public key to compute a shared secret.
- The mathematics behind this process ensures that both parties end up with the same shared secret.

d. Shared Secret Use:

- The shared secret can be used as a symmetric key for subsequent secure communication.
- As it is not transmitted over the network, it remains secure even if intercepted.

Key Operational Aspects:

1. *Modulus and Generator Selection:*

- The security of Diffie-Hellman relies on selecting appropriate values for the modulus (p) and generator (g).
- Large prime numbers for p and a primitive root modulo p for g are crucial for robust security.

b. Interception Challenge:

- Even if an adversary intercepts the public keys, the discrete logarithm problem prevents them from deriving the private keys and, consequently, the shared secret.
- The protocol's security hinges on the presumed difficulty of solving this mathematical problem.

c. Forward Secrecy:

- Diffie-Hellman provides forward secrecy, meaning that even if an adversary compromises a party's private key in the future, past communications remain secure.
- This feature is vital for maintaining the confidentiality of historical data.

d. Man-in-the-Middle Protection:

- Diffie-Hellman is vulnerable to man-in-the-middle attacks where an adversary intercepts and alters the exchanged values.
- To address this, additional mechanisms like digital signatures or certificates are often used to authenticate the communicating parties.

The Diffie-Hellman key exchange protocol is a groundbreaking advancement in the field of cryptography, providing an elegant solution to the challenge of secure key exchange over public networks. By leveraging mathematical properties and the computational complexity of the discrete logarithm problem, Diffie-Hellman ensures that even if the exchanged values are intercepted, deriving the shared secret without the private keys remains practically impossible. The protocol's reliance on openness, combined with careful selection of modulus and generator values, contributes to its robustness. While it offers forward secrecy, precautions against man-in-the-middle attacks are necessary to maximize its effectiveness in real-world applications. In summary, Diffie-Hellman stands as a key enabler for secure communications, underlining the importance of mathematical principles in modern cryptography.

2. Symmetric Key Cryptography Limitations in Real-World Internet Communications:

Symmetric key cryptography, where the same key is used for both encryption and decryption, has been a foundational technique in securing digital communications. However, as the scope and complexity of Internet communications evolve, certain limitations of symmetric key cryptography have become increasingly apparent.

Symmetric Key Cryptography Overview:

Symmetric key cryptography employs a single, shared key for both encrypting and decrypting messages. The simplicity and efficiency of this approach made it a fundamental tool in securing communication channels. In this method, both the sender and the recipient share the same secret key, ensuring that only authorized parties can access the encrypted information. This simplicity also contributes to faster processing, making it suitable for various applications.

Development and Implementation:

Symmetric key cryptography was developed to address the need for secure communication in a world where adversaries could intercept and decipher messages. Algorithms such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) have been widely used to safeguard sensitive information, including financial transactions, military communications, and more. The speed and computational efficiency of symmetric key cryptography made it a practical choice for many applications.

Despite its historical significance, symmetric key cryptography faces several challenges in the contemporary landscape of Internet communications:

1. *Key Distribution:*
- The primary challenge lies in securely distributing and managing the secret keys between communicating parties.
- As the number of participants increases, the complexity of key distribution grows exponentially, and securely exchanging keys becomes a logistical challenge.
2. *Scalability:*
- In large-scale communication networks, such as the Internet, symmetric key cryptography becomes less scalable.
- Each pair of communicating parties requires a unique key, leading to an impractical number of keys to manage in a network with numerous users.
3. *Key Exchange Overhead:*
- *The process of securely exchanging keys introduces additional overhead and complexities.*
- *Protocols like Diffie-Hellman are employed to establish shared keys securely, but these introduce computational and communication costs.*

For example, a multinational corporation needs to establish secure communication channels between its various offices worldwide. Using symmetric key cryptography, each pair of offices would require a unique key for secure communication. As the number of offices increases, managing and securely exchanging keys becomes a logistical nightmare. The sheer scale of key distribution and management challenges makes symmetric key cryptography less practical in such scenarios.

While symmetric key cryptography has played a crucial role in securing digital communications, its limitations become evident in the complexities of today's internet ecosystem. The challenges of key distribution, scalability, and key exchange overhead highlight the need for more advanced cryptographic techniques. As internet communications continue to evolve, addressing these limitations becomes essential to ensure the ongoing security and integrity of digital information.

References

Alagheband, M. R., & Atefeh Mashatan. (2022). Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives. The Journal of Supercomputing, 78(17), 18777–18824. https://doi.org/10.1007/s11227-022-04586-1

Dutkiewicz, L., Miadzvetskaya, Y., Ofe, H., Barnett, A., Helminger, L., Lindstaedt, S., & Trügler, A. (2022). Privacy-Preserving Techniques for Trustworthy Data Sharing: Opportunities and Challenges for Future Research. Data Spaces, 319–335. https://doi.org/10.1007/978-3-030-98636-0_15

Johnson, L. (2020). Security component fundamentals for assessment. Security Controls Evaluation, Testing, and Assessment Handbook, 471–536. https://doi.org/10.1016/b978-0-12-818427-1.00011-2

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: a Comparative Study. Sensors, 22(2), 538. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8778887/

Mishra, M. R., & Kar, J. (2017). A study on Diffie-Hellman key exchange protocols. International Journal of Pure and Applied Mathematics, 114(2). https://doi.org/10.12732/ijpam.v114i2.2

van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. Computer Law & Security Review, 49, 105804. https://doi.org/10.1016/j.clsr.2023.105804