Comparison the Encryption Algorithms and Design Encryption Software for the Security of SMS

Khalid Fadhil Jasim
Department of Computer Science
Cihan University-Erbil, KRG, Iraq
khalid.jassim@cihanuniversity.edu.iq

Outlines

- Introduction
- PROBLEM STATEMENT
- SYMMETRIC ENCRYPTION
- AES, Blowfish, Twofish, Triple DES
- ASYMMETRIC ENCRYPTION
- RSA, Elliptic Curve Cryptography, Diffie-Hellman
- Discussion
- Conclusions

Introduction

- **This paper provides a comparative study** to analyze some encryption algorithms for the security of SMS.
- The encryption algorithms considered in this analysis are Advanced Encryption Standard (**AES**), **Blowfish**, **Twofish**, **Triple DES**, **RSA** (Rivest – Shamir – Adleman), **Elliptic Curve Cryptography** (ECC), and **Diffie - Hellman** (DH).
- The analysis is based on three main factors: **security**, **performance**, **and compatibility**. The security analysis is based on **key length**, **security strength**, **vulnerabilities, and attacks**.

Introduction (Cont.)

- **AES and ECC are widely used and considered to be secure** and efficient for SMS encryption,
- while **hybrid encryption** can take advantage of the **strengths of** both **symmetric and asymmetric encryption** algorithms.
- **Also, we designed Encryption Software** that can be used **to protect text messages** based on some selected encryption algorithms. The selection of ciphers algorithms ultimately rely on various requirements of the SMS application in question.

PROBLEM STATEMENT

- The problem addressed in this paper **is the need for secure SMS communication.**
- **SMS messages are vulnerable** to **interception**, **unauthorized access**, **and manipulation by malicious actors**, which can lead to the compromise of sensitive information.
- **To address this problem, encryption algorithms are used to ensure the confidentiality and integrity of SMS messages.**
- **The aim of this research** is to **compare and analyze of seven encryption algorithms, the selection of the algorithm for SMS .**

SYMMETRIC ENCRYPTION ALGORITHMS FOR SMS SECURITY

- **1. Advanced Encryption Standard (AES):**
- **The AES depends on symmetric encryption,** that is known for its high level of security.
- **It uses a block cipher technique** that divides the message into fixed-sized blocks and encrypts each block separately.
- **AES supported three key sizes (128, 192, and 256 bits)** and the strength of the encryption increases with large key size [8].
- **2. Blowfish: Blowfish is symmetric encryption** algorithm that is known for its **speed and efficiency**. **It uses a block cipher.**

SYMMETRIC ENCRYPTION ALGORITHMS FOR SMS SECURITY

- **3. Twofish: This cipher relied on Block ciphers** techniques
- Supported **three secret keys (128, 192 & 256** bits).
- Twofish **possessed strong security characteristics** and has been implemented in various applications that require high levels of encryption [10].
- **4. Triple DES: Triple DES relied on symmetric encryption**
- Triple DES **uses three rounds** of encryption and supported
- **Three key sizes (56, 112, or 168 bits**).

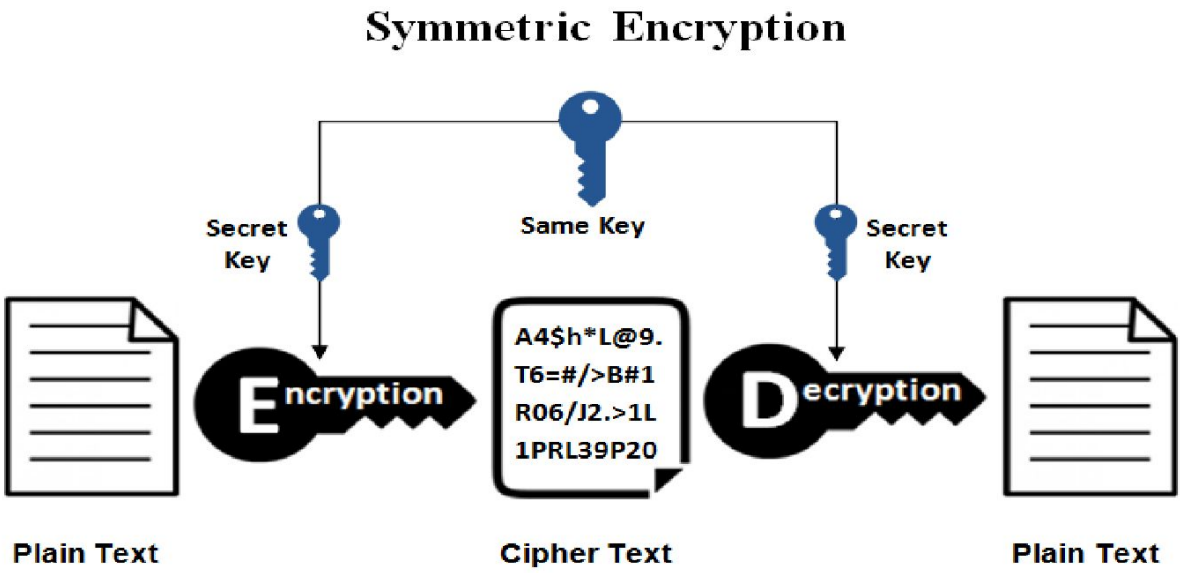

Fig. 1. Symmetric Encryption Model

ASYMMETRIC ENCRYPTION ALGORITHMS FOR SMS SECURITY

- **1. RSA (Rivest – Shamir - Adleman): The design of RSA depends** on **asymmetric encryption** technique.
- It is known for its **strong security** and **uses large prime numbers** to generate the keys.
- **RSA supports key sizes** of up to **4096 bits.**
- **Proposed in different data security** applications, such as security of **Texts** and **digital communications** [12].
- **2. Elliptic Curve Cryptography (E C C):** The design of ECC **adopts asymmetric encryption** technique.

ASYMMETRIC ENCRYPTION ALGORITHMS FOR SMS SECURITY

- **3. Diffie - Hellman (D H): Diffie - Hellman designed for key exchange in encryption systems.** This algorithm often operated in combination with symmetric encryption algorithms.
- **DH uses the same Encryption/Decryption key** (secret key) that is agreed between the first user (**sender**) and the second user (**receiver**), and usually the same key adopted for encryption and decryption processes of the messages

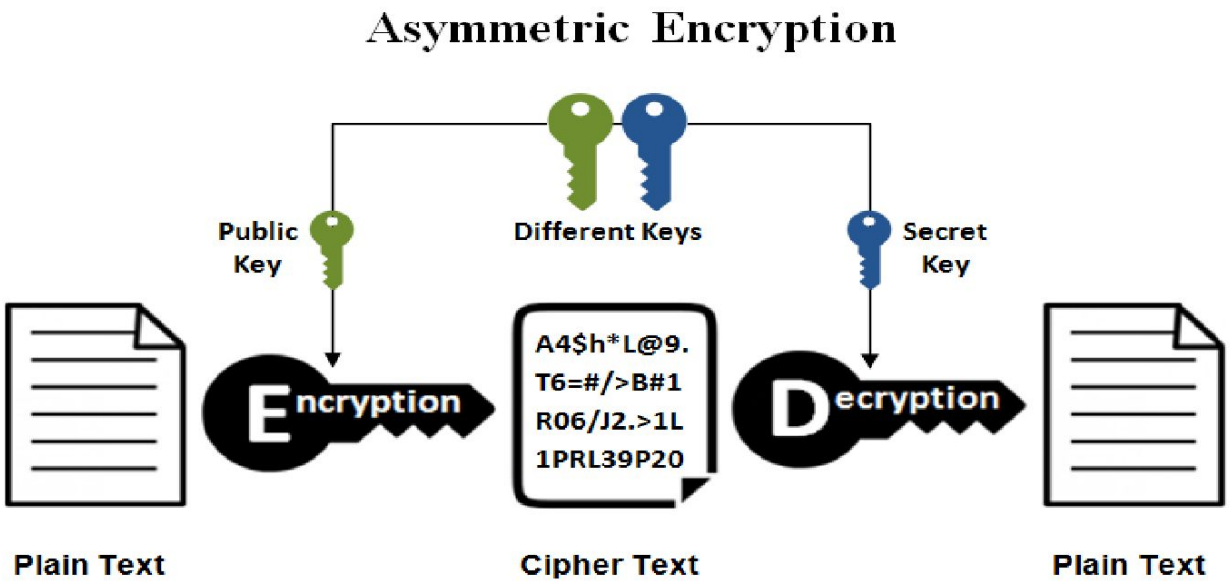

Fig. 2. Asymmetric Encryption Model

Discussion

- When it comes to **encryption algorithms for SMS security**, there are **many options** to choose
- from, each with its own strengths and weaknesses.
- we will compare seven popular encryption algorithms:
- Advanced Encryption Standard (**AES**), **Blowfish**, **Twofish**, **Triple DES**, **RSA** (Rivest-Shamir-Adleman), **Elliptic Curve Cryptography** (ECC), and **Diffie-Hellman** (DH) (Table 5).

Discussion (Cont.)

Comparison of Some Encryption Algorithms.

Encryption Algorithm	Type of Cipher	Size of Key	Block Size	Number of Rounds	Some Features
AES	Block Cipher	128, 192, 256 bits	128 bits	10, 12, 14	Excellent Security, Good performance
Blowfish	Block Cipher	32-448 bits	64 bits	16	Excellent Security, Performance less than AES
Twofish	Block Cipher	128, 192, 256 bits	128 bits	16	Excellent Security, Performance less than AES
Triple DES	Block Cipher	168,112 or 56 bits	64 bits	48	Adequate Security, Fast speed
RSA	Public Key Algorithm	1024, 2048 to 15360 bits	128 bits	1	Good Security, Low speed
ECC	Public Key Algorithm	160, 224, 256, 384, and 521 bits	Variable	1	High Security, Fast speed
DH	Public Key Algorithm	Variable	-	-	Good Security Low speed

Conclusions

- **In conclusion, the security of SMS messages is of utmost importance**, and **encryption algorithms represent secure tools** that ensuring the confidentiality and integrity of these messages.
- **In this paper, we provided a comparative analysis study of seven encryption algorithms** for SMS security: AES, Blowfish, Twofish, Triple DES, RSA, ECC, and DH.
- **The analysis was based on** three main factors: **security, performance, and compatibility**.
- **Overall, this study provides useful insights for practitioners and researchers** in the field of SMS security,

THANK YOU