A Comparative Analysis of Symmetric and Asymmetric Data Encryption Techniques with Existing Vulnerabilities

Samantha Barua Chowdhury
Department of Electrical and Computing Science, University of Alberta
Edmonton, Alberta, Canada
sc12@ualberta.ca

1 Abstract

In this proj

2 Introduction

(the first section of the paper and should include: context of the presented topic, why it is important, motivation, brief summary of presented solution, list of research contributions)

3 Background and Terminology

optional and may be spread out through the paper depending on the topic

4 Motivating/Running Example

optional, depending on the nature of the presented topic

5 Overview of Approach

a general high-level overview of the presented approach, usually accompanied with an illustrative diagram such as a workflow diagram

6 More Details about Approach

probably multiple sections

DES: Data is ciphered taking 64 bits block of data at a time and performing permutations and substitution on it with the help of secret key. The process occurs in 16 rounds, where each encrypted block is dependent on all other previous blocks. [23]
Block Size: 64 bit
Key Size: 56bit. Of them, 8 bits are used for parity, which leaves 48 bits for encryption, making it more vulnerable to attacks.
Speed:
Complexity: O(2^{55})
Attacks:

1. Since the key size determines the number of possible keys, by brute force, it would take an attacker a maximum of 2^{56} or 72,057,594,037,927,936 attempts to find the correct key. [23].
2. More vulnerable to Linear cryptanalysis than differential cryptanalysis, using 2^{43} pair of known plaintexts, though it's claimed to be quite impractical in reality.[22]

Uses:

1. Due to simplicity,it is used in smart cards, SIM cards and other embedded systems.
2. Encryption in network devices including modem, set-top boxes and routers are often done with DES. [23]

Triple DES: It uses a key bundle consisted of 3 DES keys as, **K1, K2, K3**, each with size 56 bits. The encryption algorithm is[24]:

$$ciphertext = E_{K3}(D_{K2}(E_{K1}(plaintext))) \quad (1)$$

3DES applies the DES technique 3 times to each block, thus providing an increase in key size without having to introduct a new cipher algorithm.
Block Size: 64 bit [24]
Key Size: 3x56 = 168 bits in 3TDES with keys K1, K2 and K3.
2x56 = 112 bits in 2TDES with keys K1 and K2. [1]
Speed:
Complexity:
Attacks: According to the draft guidance published by NIST on July 19, 2018, it was proposed that 3DES would be deprecated for all new applications and usage will be disallowed after 2023. [2]
Uses: The current uses of 3DES include:

1. Encryption of in-transit and at-rest data.
2. Ensuring protected credit card transaction by encrypting EMV keys. [2]

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Samantha Barua Chowdhury
Department of Electrical and Computing Science, University of Alberta
Edmonton, Alberta, Canada
sc12@ualberta.ca

IDEA(International Data Encryption Algorithm): IDEA encrypts data by 4 complete rounds and 1 half round of operations, where each complete round does the following operatons.[3]

1. Bitwise XOR
2. Addition modulo (2^4)
3. Multiplication modulo (2^4)+1

Block Size: 64 bits [4]
Key Size: 123 bits [4]
Speed:
Complexity:
Attacks:

1. In 2011, it was broken by a meet-in-the-middle attack.
2. Full 8.5 round IDEA was broken by a narroe-bicliques attack in 2012. [4]

Uses: Immune to differential cryptanalysis.

Rijndael: This algorithm is used as the AES that aims to provide resistance to all attacks with high speed and simple algorithmic design.[5]
Block Size: 128 bits [5]
Key Size: 128 bits, 160 bits, 192 bits, 224 bits and 256 bits [6]
Speed:
Complexity: It requires 9 rounds for 128 bits, 11 rounds for 192 bits and 13 rounds for 256 bits during encryption.[7]
Attacks:

1. Weak to an attack called the "Square Attack" based on matrix multiplication.
2. Theoretical vulnerability to side-channel attack and biclique attacks were presented.

However, none of these attacks were imposed on practical terms. [8] **Uses:** Requires less memory due to which it can run efficiently on computing platforms such as, smart cards, desktop systems and mobile devices. [5]

Blowfish: This algorithm is used as the AES that aims to provide resistance to all attacks with high speed and simple algorithmic design.[5]
Block Size: 64 bits.
Key Size: 32 to 448 bits of variable size. [9]
Speed: One of the fastest, except when changing keys.[10]
Complexity: For each key, encryption routine runs 522 times.[11]
Attacks: Small block size makes it more vulnerable to birthday attacks compared to the 128 bits used in AES.[12] Though key scheduling protects against brute force attacks, it has never been hacked till date. [11] **Uses:** Used in processors of mobile phones, notebook and desktop computers, for example, the product SplashID uses Blowfish. [10]

Twofish: To replace the DES algorithm, Twofish with a Feistel network was developed. In each round, half of the text block is sent through an F-function and the other half is XOR-ed.[13]
Block Size: 128 bits.
Key Size: 128 bits, 192 bits, 256 bits. [14]
Speed:
Complexity:
Attacks: Cryptanalysis include theoretical attacks with 2^64 chosen plaintexts under each key involving 2^32 work. But it is not very practical to implement [14] **Uses:**

1. Password management tools, such as, KeePass, Password Sage, use Twofish that deals with generation and storage of passwords for communication.
2. Encryption of contents of email used by PGP (Pretty Good Privacy) software.
3. Protection of files on devices using TrueCrypt encryption software.[15]
4. Used in network applications when there is little to no RAM or ROM available. [14]

6.1 Asymmetric Encryption Algorithm

6.1.1 RSA (Rivest-Shamir-Adlemann): The security of RSA is based on the difficulty of factoring large integers. It allows sending of encrypted messages without any prior exchange of secret keys and also verification of an authorised sender. [16]
Block Size:
Key Size: 1024 bits, 2048 bits, 4096 bits.
Speed:
Complexity:
Attacks:

1. Discovery of public key resulting from poor key generation by taking primes p and q too close to each other.
2. An attacker can launch side channel attacks observing the decryption of timing on target devices and using information from RSA implementation. This can be mitigated by cyptographic blinding, by adding an off-value to remove the correlation.[17]

Uses:

1. Implementation of digital signature where origin of messages is verified.
2. Encryption during information transfer. [17]

6.1.2 Diffie-Hellman): This algorithm helps to generate a shared secret such that it cannot be noticed from observing the communication. It provides encryption of traffic with the public key which ensures that finding our the key by analyzing traffic is not possible. [18]
Block Size:
Key Size: 1024 bits, 2048 bits, 4096 bits.
Speed:
Complexity:
Attacks: Vulnerable to man-in-the-middle attack for which it needs authentication implementation. [19] **Uses:**

1. Securely develop shared secrets.

2. Safe disrtibution of keys. Frequently used in security protocols such as, TLS, Ipsec, SSH, etc. [19]

6.1.3 El-Gamal): Due to the probabilistic nature of the El-Gamal cryptosystem, a single plaintext can be encrypted into many ciphertexts. This produces an expansion of size from plaintext to ciphertext in the ratio 2:1. [20]
Block Size:
Key Size: 1024 bits, 2048 bits, 4096 bits.
Speed:
Complexity:
Attacks:

1. Not secure under chosen ciphertext attack. [20]
2. Security is based on the complexity during computation of discrete logs in a large prime modulus. [21]

Uses: Establishments of secure channel for sharing of keys. [**?**]

7 Evaluation

including experimental setup, research questions, discussion of results beyond just stating some statistics such as discussing why your approach is superior for some benchmarks but not for others

8 Discussion

optional, depending on how the evaluation section of the paper is written

9 Related Work

what other papers are related to your presented topic, more importantly how your work is different or similar to those papers, as well as what limitations your work has addresses or insights it has drawn from those papers

10 Conclusion

summarize the presented problem, how you addressed it, brief summary of results, and optionally briefly discuss future work

References

[1] [n.d.]. https://www.tutorialspoint.com/cryptography/triple_des.html.
[2] [n.d.]. https://www.cryptomathic.com/news-events/blog/3des-is-officially-being-retired.
[3] [n.d.]. https://www.geeksforgeeks.org/simplified-international-data-encryption-algorithm-idea/.
[4] [n.d.]. https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm.
[5] [n.d.]. https://blog.finjan.com/rijndael-encryption-algorithm/.
[6] [n.d.]. https://crypto.stackexchange.com/questions/31632/what-is-the-difference-between-key-size-and-block-size-for-aes.
[7] [n.d.]. https://searchsecurity.techtarget.com/definition/Rijndael.
[8] [n.d.]. https://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html.
[9] [n.d.]. https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/.
[10] [n.d.]. https://www.splashdata.com/splashid/blowfish.html.
[11] [n.d.]. https://study.com/academy/lesson/blowfish-encryption-strength-example.html.
[12] [n.d.]. https://www.commonlounge.com/discussion/d95616beecc148daaa23f35178691c35.
[13] [n.d.]. https://www.drdobbs.com/security/the-twofish-encryption-algorithm/184410744.
[14] [n.d.]. https://www.schneier.com/academic/archives/1998/12/the_twofish_encrypti.html.
[15] [n.d.]. https://choosetoencrypt.com/tech/twofish-encryption/.
[16] [n.d.]. https://www.di-mgt.com.au/rsa_alg.html.
[17] [n.d.]. https://www.drdobbs.com/security/the-twofish-encryption-algorithm/184410744.
[18] [n.d.]. https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english.
[19] [n.d.]. https://doubleoctopus.com/security-wiki/encryption-and-cryptography/diffie-hellman-algorithm/.
[20] [n.d.]. https://en.wikipedia.org/wiki/ElGamal_encryption.
[21] [n.d.]. . http://homepages.math.uic.edu/~leon/mcs425-s08/handouts/el-gamal.pdf.
[22] [n.d.]. Ch-6, Data Encryption Standard. https://academic.csuohio.edu/yuc/security.
[23] [n.d.]. Network Security Data Encryption Standard. https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard. Accessed: 2020-03-27.
[24] [n.d.]. Triple DES. https://en.wikipedia.org/wiki/Triple_DES.