Best Symmetric Key Encryption - A Review

Shelveen Pandey, Mohammed Farik

Abstract: Advanced Encryption Standard (AES) is currently the leading standard for encryption which is currently used by the U.S. Government to protect sensitive data. The paper compares AES, DES, and 3DES encryptions and in light of current and future challenges.

Index Terms: AES, DES, Triple-DES, Symmetric Key Encryption, Quantum Computing

1 Introduction

In today's world, security is one of the key features of ensuring data security. The main goal of cryptography is to maintain Data Security (information from unauthorized users). Cryptography is analyzing techniques for secure communication which is preventing public or third parties reading private messages that is only projected for a particular user only. There are different ways in which data can be encrypted and it is symmetric and asymmetric. This paper will discuss symmetric encryption algorithms such as Digital Encryption Standard (DES), Triple Digital Encryption Standard (TDES) and Advanced Encryption Standard (AES) Algorithm. Symmetric algorithms uses the same key for encryption and decryption where the decryption key is derived from the encryption key. It can be classified into 2 types i.e. stream ciphers and block ciphers. The stream ciphers can be defined as encrypting a single bit of plaintext at a time whereas block ciphers takes a number of keys such as 64 bit in recent times and encrypts as a single unit only. The cipher AES-256 is also used in SSL/TLS over the internet.

2 Symmetric Key Encryption

2.1 Advanced Encryption Standard

Through research, it was identified that Advanced Encryption Standard is currently the best symmetric encryption algorithm for network security. In theory it has been said that it is not crackable (cannot be broken) since the combinations of keys are huge. The National Institute of Standards and Technology in 1999 requested for proposals for Advanced Encryption Standards. In 2001, NIST published an algorithm called Rijndale which specifies variable block sizes, key lengths which is multiple of 32 bits. AES can be said it is a replacement of Data Encryption Systems but also keeps the tradition of DES. AES specifies a fixed 128 bit block size but different key lengths ranging from 128 (10 rounds), 192 (12 Rounds) and 256 (14 Rounds) bits (NIST, 2017). AES is block cipher algorithm. It is better known as AES-128, AES-192, AES-256. It is the current US government standard and most widely used and also considered to be very secure. There has been a lot of intelligent people reviewing this algorithm and have not been able to find any significant weakness. It is the De facto standard since 2001 which supports multiple shared key strengths and lengths. It is the most commonly used symmetric key algorithm in the world.

- *Shelveen Pandey is currently pursuing Master's Degree program in Information Technology at The University of Fiji.*
- *Mohammed Farik (Member IEEE), is a Lecturer in Information Technology at The University of Fiji. E-mail: mohammedf@unifiji.ac.fj*

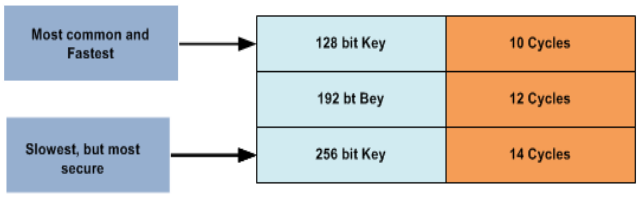

Fig. 1. *AES Key Lengths*

2.2 Digital Encryption Standard (DES)

Digital Encryption Standard (DES) was developed in 1970s by IBM which was originally a cryptographic named Lucifer. DES uses 56 keys (+8 parity bits) rather than a stream cipher and it is a block cipher which uses 64 bit blocks. In 1998, DES encrypted message was broken in 3 days. Moreover in 1999, 10,1000 desktop system managed to break DES encrypted message in less than a day. DES key size is to small and algorithm is also not effective of both hardware and software. DES was US government standard until 2001. It is considered as an obsolete Block symmetric algorithm

2.3 Triple Digital Encryption Standard (3DES)

All Triple DES is DES algorithm used 3 times where key 1 is used to encrypt a message which results in C1 cipher text, Key 2 is used to decrypt C1 which results in C2 cipher text and Key 3 is used to encrypt C2 resulting in C3 cipher text. Triple DES is not 3 times the strength of DES. Key 1 and Key 3, encryption is done whereas Key 2, decryption is done. It is an encrypt, decrypt and encrypt process with 3 separate keys. Still uses DES block cipher with 56 bit keys but when using 3 keys yields key length of 168 bits. It was used for higher level security in the 1990s but was dropped due to high overhead (slow).

Symmetric Key Algorithms

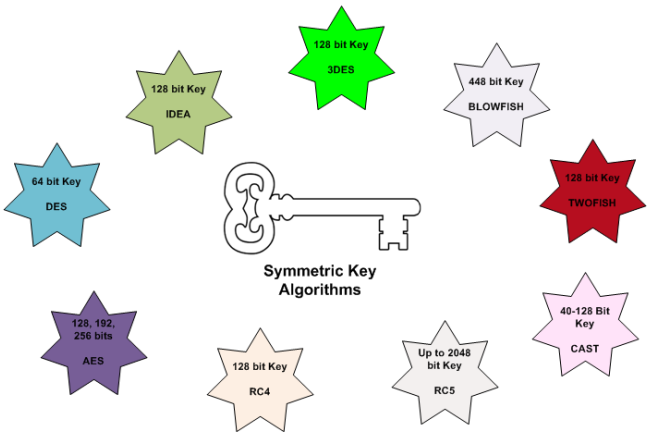

Fig. 2. *Symmetric Key Algorithms*

3 Block Cipher Modes of Operation

- Electronic Code Book (ECB) should always be used with care and only to encrypt messages with length of most of the underlying block size and with keys which are used only once. it is because without guarantees, ECB provides no modern impression of security (Smart et al., 2017). The plaintext is handled one block at time where for each block is plaintext is encrypted, the same key is used.
- Cipher Block Chaining (CBC) is the most widely used and unless it is used with a one-time key, an autonomous and random IV should be used for each message where this mode can be shown to be IND-CPA secure if the underlying block cipher is secure (Smart et al., 2017).
- Cipher feedback (CFB) is where the input is processed bits at a time and the previous cipher text is used as input to the encryption algorithm to produce pseudorandom output which is therefore XORed with the plaintext to produce next unit of the cipher text (Stalling, 2017).
- Output Feedback (OFB) is where full blocks are used. It is similar to Cipher Feedback except the input to the encryption algorithm is the preceding encryption out (Stalling, 2017).
- Counter (CTR) is where each block of plaintext is XORed with an encrypted counter which is incremented for each following block (Stalling, 2017).

4 Application areas in networks

There are several archive as well as compression tool and some are RAR, WinZip, UltraISO, Amanda Backup. Some of the file encryption used is Gpg4win whereas encrypting file systems use AES (E.G. self encrypting drives) such as NTFS. It is very important to secure data on a drive. For disk or partition encrypt, AES is used for Bitlocker, DiskCryptor, LUKS, VeraCrypt. For wireless technologies, IEEE 802.11i which is an amendment of IEEE 802.11 uses AES-128 in CCM mode. It is used in WPA2, when moved from WEP encryption which is used in wireless networks.

5 Hardware and Software Supporting AES

There are a lot of hardware's and software's supporting AES. These include C/ASM Library (Libgcrypt), C++ Library (Botan) (Wikipedia, 2017), C# /.Net (Bouncy Castle Crypto Library, Java, Pythoon, JavaScript, LabVIEW. Arista Networks (EIP-165 crypto core Version 1.0 Firmware), Ciena Corporation (Ciena 8700 Packetwave Platform Version 8.5), OpenSSL Validation services (Open SSL FIPS Object Module Ver. 2.0.16), Trustonic (TRICX Ver. 1.0), Hewlett Packard Enterprise Company (iLO Hardware Crypto Library), HGST (NIST, 2017), a Western Digital (Marvell XTS-AES Media Encryption Engine Ver. 3.1), A10 Networks Inc (A10 Networks SSL FIPS Library Ver. 2.0.0), ARM Ltd (wpan01_aes_top Ver. 1.4), Tintri (Tintri Cryptographic Module Ver. 1.0), Gemalto (MultiAppIDV4.0 Cryptographic Library), Persistent Systems LLC (Wave Relay Cryptographic Library Ver. 2.0), WolfSSL Inc (WolfCrypt Ver. 3.9.0 EDMI. 2), Huwaei technologies (Openssl Ver. 1.0.2h), Ciena Corporation (Ciena Waveserver Ver. 1.4), ALE (Alcatel Lucent Enterprise) (Common Criteria Evaluation [CCE] Certification for ALE AoS OmniSwitch (OS6900 PowerPC P2040 ECDSA-GCM-TDES-RSA-PSS Ver. A OS 8.3.1.R01). AMD and INTEL processors also include AES instructions whereas for IBM zSeries mainframes, AES is installed on KM assembler of opcodes. SPARC S3 which also includes AES on SPARC T4 and SPARC T5 systems.

6 AES supported malware

Alcatraz Locker was first detected in mid November 2016 which is a Ransomware strain and uses AES 256 encryption combined with Base64 encoding (AVAST, 2017). CryptoMix (well known as CryptFile2 or Zeta) is a Ransomware strain which was initially covered in March 2016. CryptoShield which is a new variation of CryptoMix was detected in early 2017. A remote serer is used to download a unique encryption key where AES256 encryption is used by both variants to encrypt files (AVAST, 2017)

7 Current & Future Challenges

Encryption is basically not dead but will be the main savior in the near future and keeping with the various market will be the key. Providing workable solutions which will be interoperability in mobile telecommunications and heterogeneous environments will be crucial. Some of the driving forces of encryption are email privacy and regulatory requirements, expanding enterprise, user mobility, communication appliances and storing and retrieving of information from cloud (Dunkelberger, 2017). There has been a lot of financial losses for corporations and a lot of these attacks are known to be linked with unauthorized access. Millions and millions of dollars are spent in retrieving confidential information once it has been stolen and a lot of government agencies are working to find ways in ways to prevent this. There is a lot of communication appliances (Notebooks, Mobile phones, PDA's Personal Information Managers) to name a few which is assisting individuals and organizations communicate as well as store information. A lot of concern now is to ensure how safe is information while it is residing in the device as well as how secure is it when information is being transmitted. Internet Protocol Security (IPsec) is protocols for securing Internet communications at network layer which operates within Internet protocol (IP) which is frequently used in Virtual Private Networks where both parties share key to securely access business networks (NIST Special Publication 800 - 57 Part 3, 2015). IPsec provides cryptographic functions to both IPv4 and IPv6. NISTs Recommendation for Key Management Part 1: General (NIST SP800-57 P1. R4., 2016) states that 256 bit key is secure beyond year 2031. The report also mentioned development in Quantum computing would be a great threat so the theory is regarding the safety of encryption mentioned beyond year 2031 must be looked into.

8 Quantum Computing

Quantum computing uses quantum bits or qubits rather than the traditional computers using 0's and 1's. Quantum bits can store much more information than the traditional 1 or 0. Google and NASA (Beall, 2017) found a D-wave quantum computer that was 100 million times faster than a standard computer system. It also stated that what a normal computer could do in 10,000 years would now just take seconds. Some reports regarding Quantum computing funding is being done (Pearce, 2016) by Commonwealth bank committing $10 million over 5 years as well as Telstra in 2015 would invest $10 million in the center for Quantum Computation and Communication Technology. Research also suggests that major threat to security now is the evolution of Quantum Computing. According to (Anja, 2017) all Asymmetric standard algorithms will be breakable such as RSA, Elliptic curve, Diffie-Hellman and has also mentioned symmetric key with 128 bits can be broken in 264 iterations. After doing research on the

current encryption standard and Quantum computing and the risk involved, we would suggest Quantum developers and encryption security experts to get together and discuss a way forward where security is maintained and the evolution of Quantum computing is a safe evolution for the ICT community since looking at the advancement with Quantum computing, AES encryption is also not safe. Research also suggests that major threat to security now is the evolution of Quantum Computing. Further research can be done to have Quantum proof encryption standards.

9 Conclusion

Through this research it can be concluded that AES is the best algorithm at present. There are other symmetric algorithms but they all have their limitations. It has also been proven that AES is the standard encryption for US government which has been approved by National Security Agency. Many modern methods of symmetric key encryption utilize both stream and block schemes. An understanding of encryption can assist individuals in securing private data as well. With the evolution of Quantum computers, there is a risk to the encryption and suggestions mentioned is for Encryption security experts as well as Quantum developers to get together and get a solution to maintain security as security has been and will always be the main priority.

References

[1] Anja. (2017, February 9). Quantum Computers - a Threat for PKI? Retrieved May 25, 2017, from securosys: https://www.securosys.ch/quantum-computers-threat-pki

[2] Avast. (2017). Free Ransomware Decryption Tools. Retrieved May 02, 2017, from Avast: https://www.avast.com/ransomware-decryption-tools

[3] Beall, A. (2017, March 23). Inside the weird world of quantum computers. Retrieved May 24, 2017, from WIRED: http://www.wired.co.uk/article/quantum-computing-explained

[4] Dunkelberger, P. (2017). The Future of Encryption. PGP Corporation.

[5] NIST. (2001). ADVANCED ENCRYPTION STANDARD (AES). Gaithersburg: Federal Information Processing Standards Publication 197.

[6] NIST. (2017). Advanced Encryption Standard Algorithm Validation List. Retrieved April 30, 2017, from http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html

[7] NIST SP800-57 P1. R4. (2016). Recommendation for Key Management Part 1: General. National Institute of Standards and Technology. National Institute of Standards and Technology.

[8] NIST Special Publication 800-57, P. 3. (2015). Recommendation for Key Management. National Institute of Standards and Technology.

[9] Pearce, R. (2016, June 02). Bank's investment in quantum computing. Retrieved May 24, 2017, from Computerworld: https://www.computerworld.com.au/article/600879/behind-commonwealth-bank-investment-quantum-computing/

[10] Smart, N. P., Rijmen, V., Warinschi, B., & Watson, G. (2013). Algorithms, Key Sizes and Parameters Report . Heraklion: European Union Agency for Network and Information Security Agency .

[11] Stallings, W. (2011). NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS (FOURTH ed.). (Michael, Ed.) Pearson Education, Inc.

[12] Wikipedia. (2017). AES implementations. Retrieved April 24, 2017, from Wikipedia: https://en.wikipedia.org/wiki/AES_implementations

[13] Beall, A. (2017, March 23). Inside the weird world of quantum computers. Retrieved May 24, 2017, from WIRED: http://www.wired.co.uk/article/quantum-computing-explained