Cryptographic Algorithms and Protocols

Chapter · November 2021

DOI: 10.1201/9781003138037-2

1 author:

Mohammad Khalid Imam Rahmani
Saudi Electronic University
62 PUBLICATIONS **378** CITATIONS

SEE PROFILE

Cryptographic Algorithms and Protocols

Mohammad Khalid Imam Rahmani
Department of Computer Science,
College of Computing and Informatics,
Saudi Electronic University, Riyadh 11673, Saudi Arabia
m.rahmani@seu.edu.sa

https://orcid.org/0000-0002-1937-7145

Abstract
Cryptography facilitates sharing of sensitive contents among the intended parties across any insecure network channels and prevents unintended recipients from knowing the secret information in the contents. Efforts are made to create tools for information hiding with modern cryptographic algorithms and security protocols. The technology is growing rapidly with the public key and private key cryptography for securing the sensitive information of organizations and performing online tasks with trusted parties. Many state-of-the-art cryptographic algorithms and protocols have been developed. For a promising researcher of this field, knowledge, and understanding of the popular key algorithms and protocols are essential for developing a solid foundation for selecting a correct research direction. This chapter is presenting the key algorithms and protocols used in Cryptography. The objective is to provide a technical description of key algorithms and protocols along with a basic understanding of the field.

Keyword
Cryptography, Encryption, Decryption, Cryptographic Algorithms, Cryptographic Protocols

1 Introduction

In the rapidly growing digitization initiatives in each Government and private department, security of their valuable contents is a major issue. The information security assurance is a key to win the trust of users for the safety and secrecy of the data being shared by different parties over the Internet or any network channel (Bourgeois, 2014). The economical availability of good quality communication hardware and software tools has created tremendous opportunities for exploring more effective and efficient security techniques for securing the information of organizations (Soomro et al., 2016). Two contemporary technologies for the purpose are cryptographic algorithms and cryptographic protocols (Gupta, et al., 2016).

The reason why unauthorized parties become successful in reading secret information is that they have opportunities to access and reveal the secret information from the secured systems (Bourgeois, 2014) due to the vulnerability in such systems. As a result, attackers can misuse or modify the information, reveal the secret information to some dangerous parties, wrongful representation to some organization, or making a plan for some more harmful activities (Tsai and Chen, 2013). Cryptography provides a solution to this problem.

Cryptography uses cryptographic algorithms and protocols to make it difficult for any unauthorized users to reveal any restricted information (Mandal et al., 2012).

The main objective is to understand available tools and techniques and the importance of secure transmission of data while achieving authenticity, confidentiality and other security principles so that attacks can be prevented and secrecy of data can be ensured. Other objectives are: (1) To go through existing cryptographic techniques and to identify strong and weak points in the field of cryptography, (2) To have an insight into Cryptographic algorithms and protocols, and (3) To explore application areas of Cryptography.

The cryptographic algorithms are described. The requirements of cryptographic protocols are discussed. Along with the conclusion, some application areas of cryptography and research trends in information security have been explored.

2 Preliminaries

Cryptography is an ancient Greek word in which 'crypt' means 'hidden' and 'graphy' means 'writing'. It is the science and art of attaining security by transforming original messages into unintelligible forms (Rosenheim, 2020) or providing immunity against unauthorized access. Cryptographic algorithms are used to encode the messages before securely sharing the information through a network so that it becomes extremely tough for an unauthorized person to reveal secret details from the message.

The important components used in cryptography are summarized in Figure 1.1:

1. Plaintext and Ciphertext: The original message which the sender wants to share is called plaintext. At the sender end, the plaintext is transformed into a secured form with an encryption algorithm. It is called a ciphertext. At the receiver end, a decryption algorithm is used to transform the ciphertext back into plaintext.

2. Cipher: The term cipher is used to refer to encryption and decryption algorithms. The cipher is used for different categories of algorithms in cryptography.

3. Key: A key refers to a number that an encryption/decryption algorithm uses to transform a plaintext into ciphertext or vice-vera. To generate a ciphertext from the plaintext, an encryption key and an encryption algorithm are required. To obtain the original message from back the ciphertext, a decryption key, and a decryption algorithm are required.

4. Alice, Bob, and Eve: It is customary to understand three typical characters in Cryptography which represent either computers or processes. Alice is the sender of secured data to the receiver Bob. Eve is the person who somehow intercepts the communication channel connecting Alice and Bob. Eve is able to either decipher the original message or sends her own disguised messages to Bob.

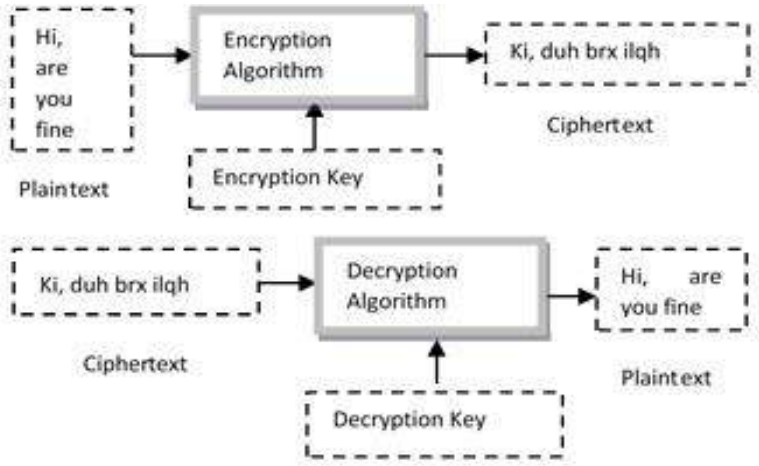

Figure 1.1. Basic Model of Cryptography. Figure by the author

Cryptographic goals

Understanding Cryptographic goals are essential for analyzing security issues for information systems, utilizing capabilities of Cryptographic systems up to their full extents and also for measuring the strength and weaknesses of Cryptographic algorithms and protocols. There are four cryptographic goals described below:

- **Confidentiality** is about ensuring access to information only to the authorized parties. Confidentiality ensures privacy. There are many approaches to implement confidentiality like from physical lock&key protection, passwords, and mathematical algorithms to make data unintelligible.
- **Data integrity** is about safeguarding the information systems from any unauthorized change of data. To ensure data integrity, the system must be able to detect any manipulation of data by unauthorized parties.
- **Authentication** ensures the identification of parties trying to access data.
- **Nonrepudiation** is a task that prevents a party from denying previous commitments or actions. If a dispute arises certain third-party intervening is required to resolve it.

Any Cryptography system must address all the four goals in practice (Stinson and Paterson, 2018) because the objective of Cryptography is to discover any unwanted trespassing and deny its consequences like theft of information or any kind of fraudulent activities.

The most fundamental terms in Cryptography are enciphering (encryption) and deciphering (decryption). Encryption transforms plaintext into ciphertext and Decryption converts the ciphertext back into plaintext (Rosenheim, 2020). A special number known as a key is used with the enciphering and deciphering processes.

3 Cryptographic Algorithms

The cryptographic algorithms are the set of mathematical and logical steps essential for transforming secret information into an encrypted cipher and for getting back the original information from the encrypted cipher. There are so many algorithms that are used in Cryptography. The most important ones are being described here.

Types of Encryption Algorithms

Symmetric Key Algorithms: In symmetric key algorithms, the sender encrypts the plaintext and the receiver decrypts the ciphertext with a single secret key. They are also called secret key or private key algorithms. The key must be secured from unauthorized access because any party having the key can decrypt the sensitive data or even encrypt new data and can make a claim that it was originated from a sender. These algorithms are faster than asymmetric key algorithms. Therefore, they are used for larger data sizes. The shared key should be available to only the actual sender and receiver. The issue of key sharing between the sender and receiver causes many challenges. The diagram in Figure 1.2 shows the process of encryption/decryption for symmetric Cryptography.
The most common encryption techniques are described below:
Data Encryption Standard or DES is the first encryption algorithm released by NIST. A team from IBM developed it in 1974. It was adopted as a national standard in 1997. It has both key size and block size of 64 bits. Only the 56 bits of 64 bits are used by the algorithm (Standard et al., 1999). The remaining 8 bits are set aside for the parity of other bits and are discarded later. DES uses Feistel network. It served as a standard for securing secret commercial and unclassified data.

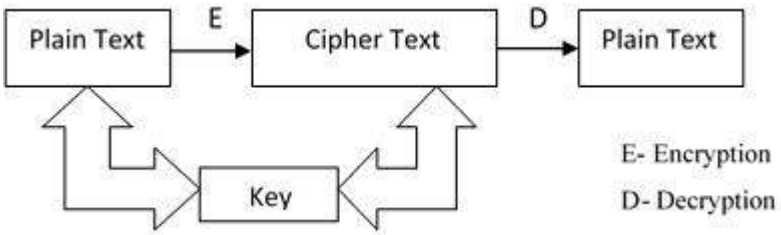

Figure 1.2. Symmetric Key Cryptography. Figure by the author

Triple DES or TDEA is an extension of DES. It has 192 bits of key size with block size of 64 bits. The encryption method differs from the original DES. It applies 3 times to enhance the level of encryption and the average safe time. TDEA is slower than other block cipher methods (Kelsey et al., 1996). Being a strong encryption algorithm, it finds its application in the banking industry.
RC2 uses 64 bits block ciphers with key sizes from 8 to 128 bits. It uses 18 rounds of two different types called MIXING (16 rounds) and MASHING (2 rounds).
Blowfish uses 64 bits block cipher meant for replacing the DES algorithm. It applies key sizes from 32 to 448 bits. Blowfish takes 14 or lesser rounds.

Advanced Encryption Standard (AES) is a symmetric key encryption/decryption algorithm based on block cipher. It supports block size of 128 bits and key sizes of 128, 192, or 256 bits; default 256 bits. Joan Daemen and Vincent Rijmen developed it to become the winners of a competition conducted by NIST to replace DES. Consequently, the US Government adopted AES superseding DES. AES is a special case of the Rijndael algorithm which can select block/key size of 128, 160, 192, 224, or 256 bits. NIST published it as FIPS 197 on 26th November 2001. AES Standards have been summarized in Table 1.1 (Dworkin et al., 2001). In the case of 128 bits key length, the number of rounds is 10 (9 processing rounds and 1 extra round performed at the end of encipherment). In the case of 192 bits key size, the number of

rounds is 12. In the case of 256 bits key length, the number of rounds is 14. Encryptions performed by AES (Zhang et al., 2021) are fast and flexible. It is suitable for different platforms. This algorithm uses the substitution-permutation network. Its performance is good in software and hardware. AES uses a Non-Feistel network.

AES Standards	Key Size (in bits)	Block Size (in bits)	Number of Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

Table 1.1. Summary of AES Standards

Each round is carried out in four steps:
Substitute bytes: It involves a non-linear substitution of one byte with another according to a lookup table. It ensures non-linearity.
Shift rows: It involves in transposition of the last three rows and are shifted cyclically for a certain number of steps.
Mix columns: A linear operation carried out on the columns of the state. It combines the four bytes of each column. Shift rows and mix columns provide diffusion.
Add Round key: A subkey is involved for combining its each byte with the corresponding bytes of the state.

Asymmetric Key Algorithms: In asymmetric key algorithms, separate keys are used to encrypt and decrypt the data. One key is the public key used for encryption which must be shared with the senders. Another key (private key), used for decrypting, must be kept secret. Therefore, they are also known as public-key algorithms. Asymmetric encryption algorithms like RSA (Zhang et al., 2021) cannot encrypt large size of data. The diagram in Figure 1.3 illustrates the mechanism of encryption/decryption in public key algorithms:

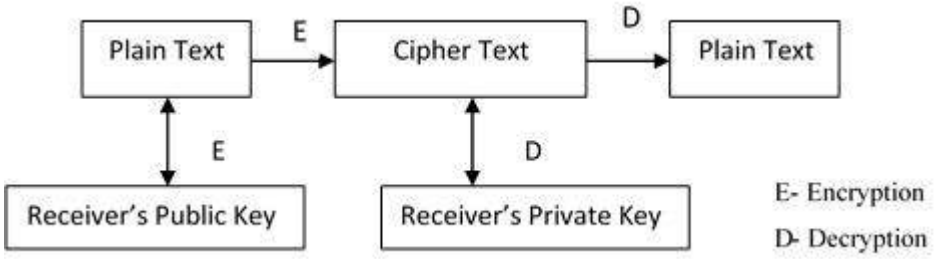

Figure 1.3. Asymmetric Key Cryptography. Figure by the author

The messages can be encrypted with both the public key and the private key. For decryption, only the private key can be used. These encryption systems ensure the goal of confidentiality because a message encrypted by any sender using the receiver's public key can only be decrypted by the receiver's paired private key. In digital signature schemes of public-key cryptography sender authentication (Sharma and Singh, 2021), integrity and nonrepudiation are ensured (Forouzan, 2011). Asymmetric algorithms are slower but they do not face the issue of key distribution. Some asymmetric algorithms are Diffie-Hellman, RSA, and DSA etc.

Rivest, Shamir, and Adleman (RSA) is one of the popular public key algorithms used for encryption purpose and also as digital signatures.

Digital Signature Algorithm

Digital Signature Algorithm (DSA) is also a public key algorithm that is used only for digitally signing documents. This scheme is suitable for achieving authentication before a message or documents are shared (Forouzan, 2011). Receiving a digitally signed document, the recipient becomes confident that the sender was a genuine one and the document was not altered during the transmission. Digital signatures are applied in software distribution, financial transactions, and for documents that might be tampered with. To verify the document the receiver performs the following steps:

1. Decrypts the digital signature using the sender's public key to read the message.
2. Generates a message digest for the receiver's message using the same algorithm used by the sender.
3. If both message digests do not match, the sender's message digest is considered to be compromised.

Hash functions

Hash functions or one-way functions are used in public-key cryptography for implementing protocols (Alawida et al., 2021). Hash functions do not need any key. They are easily computable but harder to reverse. For example, f(x) can be computed easily but the computation of x from f(x) will take many years even for all the computers of the world collectively. The value of f(x) is a fixed-length hash value computed out of x which is the plaintext. Neither the contents of the plaintext nor its length can be obtained. Hash functions are used to verify the integrity of the documents and encryption of passwords. Even a small bit of change in the contents can be easily detected because the hash values of the two versions will be absolutely different.

4 Cryptographic protocol

Cryptography analyses the issues of integrity, authentication, privacy, and nonrepudiation. Cryptographic algorithms are having academic importance (Schneier, 2007). Application of these algorithms alone cannot guarantee to achieve the goal of Cryptography. Well-defined policies and agreements between the parties involved in the communication are also required in order to make Cryptography a reliable technology for achieving its goals so that it can solve real problems in completing online tasks between trusted parties.

A cryptographic protocol is a distributed algorithm designed to precisely describe the interactions between two or more parties with the objective of implementing certain security policies. It follows some series of steps in exact sequence. Every step must be completely executed without any alteration in the agreed-upon sequence. It must be complete and able to finish a task. At least two parties are required. Any single party executing a series of steps to complete a task is not a protocol. Every party must know, understand, and follow it. They must not be able to do something beyond the specified agreement.

A cryptographic protocol uses some cryptographic algorithm to achieve the goal.

Arbitrated Protocols
Arbitrated protocols use a trusted third party called an arbitrator. The arbitrator has no vested interest and cannot favor any of the involved parties. Such protocols are used to complete tasks between two or more parties not trusting each other.

Adjudicated Protocols
The arbitrated protocols are implemented with two subprotocols to reduce the cost of third-party involvement. Some non-arbitrated protocol is used in the first level which is executed for each task. In the second level, an arbitrated protocol is used which is executed only in case of disputes occur between the involved parties during the task.

Self-Enforcing Protocols
These protocols require no arbitrator to complete tasks or to resolve disputes. The protocol itself ensures that there is no dispute between the involved parties. One party can detect whenever the other party is trying to play smart and the task is stopped immediately. It is ideal that every protocol should be self-enforcing.

Similar to the attacks on Cryptographic algorithms and techniques, protocols can also be attacked by the cheaters.

Types of Protocols

Key Exchange Protocols
A key exchange protocol is required for two parties to reach an agreement for a shared secret key. Either one party can authenticate the other or both parties can authenticate each other. The protocol can agree for the generation of a random key. One party can generate the key and send it to another party or both parties can participate in the key generation.

Diffie-Hellman key exchange
This protocol is used by the involved parties to agree on a shared key by exchanging messages through a public channel. Therefore, the key is not revealed to any unauthorized party. This is protected only against passive attacks.

Identification and Authentication Protocols
Identification protocols are required to ensure the identity of both parties when they are online for a task. Genuine possession of their private keys needs to be verified. The level of identification by the protocols may be judged with three levels: (1) Who is he? – Biometrics is used, (2) What he possesses? –Some hardware gadgets can be used, (3) What he knows? – Secret keys or passwords are used.
Some popular protocols are zero-knowledge protocol, Schnorr Protocol, Guillou-Quisquater protocol, witness hiding identification protocols, etc.

Using Password Authentication
In absence of any digital signature scheme the two parties can share a password that is comparatively less powerful.

Protocol using Digital Signatures
Digital signatures-based protocols are used to protect against the active attacks by authenticating the two parties.

5 Issues in Cryptography

In symmetric cryptography, if the key is lost, communication cannot be completed. This creates an issue of secure key distribution with possibly involving either the sender and the receiver to communicate directly or via a trusted third party or communicating via an existing cryptographic medium (Sharma et al., 2021). The issue of key distribution is to be dealt with delicately: keys must be stored, used, as well as destroyed securely.

Cryptography only transforms plaintext but never hides it (Rahmani et al., 2014). One weakness of Cryptography is if somehow any third party detects the presence of an encrypted message, it can make attempts to break into it out of curiosity. Sometimes curiosity feeds the cat. As a consequence, it can reveal the secrecy, modify or misuse the information.

6 Conclusion

For a secret communication, secrecy of messages must be ensured. In this book chapter, a short account of the techniques and mechanisms for information security for sharing secret information between two or more parties, are provided. A detailed description of both cryptographic algorithms and protocols is given.

Future works in the field need to be selected for exploring some useful techniques that can enhance the security of information and enhance the ease and confidence of sharing secret information in online mode. Securing the secret message is the primary issue. A study of Cryptanalysis is also required to test the information security systems with more stringent cipher breaking techniques in a vulnerable environment. Thirdly, we need to develop an information security infrastructure framework with modern cryptographic tools and techniques that will save time and increase the capacity of hidden secret messages for sharing confidential information with online trusted parties.

References

[1] David Bourgeois. Information systems for business and beyond. The Saylor Foundation, 2014.

[2] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. “Information security management needs more holistic approach: A literature review”. In: International Journal of Information Management 36.2 (2016), pp. 215–225.

[3] Brij Gupta, Dharma P Agrawal, and Shingo Yamaguchi. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global, 2016.

[4] Ming-Hong Tsai and Chaur-Chin Chen. “A study on secret image sharing”. In: Proceedings of the 6th International Workshop on Image Media Quality and its Applications, Tokyo, Japan. Citeseer, 2013.

[5] Akash Kumar Mandal, Chandra Parakash, and Archana Tiwari. “Performance evaluation of cryptographic algorithms: DES and AES”. In: 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science. IEEE, 2012, pp. 1–5.

[6] Shawn James Rosenheim. The cryptographic imagination: secret writing from Edgar Poe to the Internet. JHU Press, 2020.

[7] Douglas Robert Stinson and Maura Paterson. Cryptography: theory and practice. CRC press, 2018.

[8] Data Encryption Standard et al. “Data encryption standard”. In: Federal Information Processing Standards Publication (1999), p. 112.

[9] John Kelsey, Bruce Schneier, and David Wagner. “Key-schedule cryptanalysis of idea, g-des, gost, safer, and triple-des”. In: Annual international cryptology conference. Springer, 1996, pp. 237–251.

[10] Dworkin, M., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E. and Dray, J. (2001), Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.197 (Accessed March 28, 2021)

[11] Zhang, X. Hu, J. Li, H. Guan, A comprehensive test framework for cryptographic accelerators in the cloud, Journal of Systems Architecture 113 (2021) 101873.

[12] Sharma, A. Singh, Privacy preserving on searchable encrypted data in cloud, in: Advances in Communication and Computational Technology, Springer, 2021, pp. 847–863.

[13] Behrouz A. Forouzan, Cryptography and Network Security, 2nd Edition, Publisher McGraw-Hill Education (India) Pvt Limited, 2011.

[14] M. Alawida, A. Samsudin, N. Alajarmeh, J. S. Teh, M. Ahmad, et al., A novel hash function based on a chaotic sponge and dna sequence, IEEE Access 9 (2021) 17882–17897.

[15] Schneier, Applied cryptography: protocols, algorithms, and source code in C, john wiley & sons, 2007.

[16] Sharma, S. Jain, B. Chandavarkar, Nonce: Life cycle, issues and challenges in cryptography, in: ICCCE 2020, Springer, 2021, pp. 183–195.

[17] Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal, A Crypto-Steganography: A Survey, International Journal of Advanced Computer Science and Applications, 5.7, 2014, pp. 149-155.