Cryptography and State-of-the-art Techniques

Mohiuddin Ahmed[1], T. M. Shahriar Sazzad[2] , Md. Elias Mollah[3]

[1,2,3] Computer Science & Engineering Department, Green University of Bangladesh, Dhaka-1207, Bangladesh

Abstract

Cryptography is an indispensable tool for protecting information in computer systems. Modern cryptography has strong relation with various disciplines like mathematics, computer science and electrical engineering along with data security. There are tremendous applications of cryptography in recent times, like passwords, e-commerce, smart cards etc. In this paper we will focus on the state-of-the-art techniques and their efficiencies.

Keywords: *Cryptography, Cipher, Symmetric-Key, Public-key Data security, Authentication.*

1. Introduction

Cryptography (or cryptology; from Greek κρυπτός, "hidden, secret"; and γράφειν, graphein, "writing", or -λογία, -logia, "study", respectively) [1] is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was almost synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography follows a strongly scientific approach and designs cryptographic algorithms around computational hardness assumptions, making such algorithms hard to break by an adversary. It is theoretically possible to break such a system but it is infeasible to do so by any practical means. These schemes are therefore computationally secure. There exist information-theoretically secure schemes that provably cannot be broken—an example is the one-time pad—but these schemes are more difficult to implement than the theoretically breakable but computationally secure mechanisms.

Cryptology-related technology has raised a number of legal issues. In the United Kingdom, additions to the Regulation of Investigatory Powers Act 2000 requires a suspected criminal to hand over their encryption key if asked by law enforcement. Otherwise the user will face a criminal charge. The Electronic Frontier Foundation is involved in a case in the Supreme Court of the United States, which will ascertain if requiring suspected criminals to provide their encryption keys to law enforcement is unconstitutional. The EFF is arguing that this is a violation of the right of not being forced to incriminate oneself, as given in the fifth amendment.

Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called cipher text) [3]. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. This is a secret parameter (ideally

known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

Some use the terms cryptography and cryptology interchangeably in English, while others (including US military practice generally) use cryptography to refer specifically to the use and practice of cryptographic techniques and cryptology to refer to the combined study of cryptography and cryptanalysis [4] [5]. English is more flexible than several other languages in which cryptology (done by cryptologists) is always used in the second sense above. In the English Wikipedia the general term used for the entire field is cryptography (done by cryptographers).

2. State-of-the-art Approaches

In this section we focus on Public-key cryptography, SAFER (Secure And Fast Encryption Runtime) and Symmetric-key cryptography.

2.1 Public-key cryptography

Public-key cryptography refers[6] to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. Neither key will do both functions. One of these keys is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Although in this latter case, since encrypting the entire message is relatively expensive computationally, in practice just a hash of the message is encrypted for signature verification purposes.

This cryptographic approach uses asymmetric key algorithms, hence the more general name of "asymmetric key cryptography". Some of these algorithms have the public key/private key property; that is, neither key is derivable from knowledge of the other; not all asymmetric key algorithms do. Those with this property are particularly useful and have been widely deployed, and are the source of the commonly used name. The public key is used to transform a message into an unreadable form, decrypt able only by using the (different but matching) private key. Participants in such a system must create a mathematically linked key pair (i.e., a public and a private key). By publishing the public key, the key producer empowers anyone who gets a copy of the public key to produce messages only s/he can read -- because only the key producer has a copy of the private key (required for decryption). When someone wants to send a secure message to the creator of those keys, the sender encrypts it (i.e., transforms it into an unreadable form) using the intended recipient's public key; to decrypt the message, the recipient uses the private key. No one else, including the sender, can do so.

Thus, unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one, or more, secret keys between the sender and receiver. These algorithms work in such a way that, while it is easy for the intended recipient to generate the public and private keys and to decrypt the message using the private key, and while it is easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to figure out the private key based on their knowledge of the public key. They are based on mathematical relationships (the most notable ones being the integer factorization and discrete logarithm problems) that have no efficient solution.

The use of these algorithms also allows authenticity of a message to be checked by creating a digital signature of a message using the private key, which can be verified using the public key.

2.2 SAFER

The first SAFER cipher was SAFER K-64, published by Massey in 1993, with a 64-bit block size. The "K-64" denotes a key size of 64 bits. There was some demand for a version with a larger 128-bit key, and the following year Massey published such a variant incorporating new key schedule designed by the Singapore Ministry for Home affairs: SAFER K-128. However, both Lars Knudsen and Sean Murphy found minor weaknesses in this version, prompting a redesign of the key schedule to one suggested by Knudsen; these variants were named SAFER SK-64 and SAFER SK-128 respectively — the "SK" standing for "Strengthened Key schedule". Another variant with a reduced key size was published, SAFER SK-40, to comply with 40-bit export restrictions.

There are two more-recent members of the SAFER family that have made changes to the main encryption routine,

designed by the Armenian cryptographers Gurgen Khachatrian and Melsik Kuregian in conjunction with Massey. SAFER+ was designed in 1998 which has a block size of 128 bits. In the year 2000, SAFER++ was submitted to the NESSIE project in two versions, one with 64 bits, and the other with 128 bits [7].

All of these ciphers of SAFER K and SAFER SK generation use the same round function consisting of four stages : a key-mixing stage, a substitution layer, another key-mixing stage, and finally a diffusion layer. In the first key-mixing stage, the plaintext block is divided into eight 8-bit segments, and sub keys are added using either addition modulo 256 (denoted by a "+" in a square) or XOR (denoted by a "+" in a circle). The substitution layer consists of two S-boxes, each the inverse of each other, derived from discrete exponentiation (45x) and logarithm (log45x) functions. After a second key-mixing stage there is the diffusion layer: a novel cryptographic component termed a Pseudo-Hadamard transform (PHT). The PHT was later used in the Twofish cipher .

SAFER+ is a substitution-linear transformation network based on the SAFER family of ciphers. There are 8, 12, or 16 rounds, depending on the key size, plus an output transformation after the final round. The round function consists of key-controlled substitution on the sixteen bytes of the data block followed by an invertible linear transformation on the entire data block. The substitution function acts on each individual byte with a combination of key addition, key XOR, and either a fixed permutation or its inverse. The permutation corresponds to discrete exponentiation of a fixed generator in the multiplicative group of integers modulo 257. The linear transformation is generated by a combination of the Pseudo-Hadamard Transform matrix and the “Armenian Shuffle” permutation. The decryption routine is derived from the encryption routine by inverting each step.

2.3 Symmetric-key Cryptography

The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern embodiment of Alberti's polyalphabetic cipher: block ciphers take as input a block of plaintext and a key, and output a block of cipher text of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the modes of operation and must be carefully considered when using a block cipher in a cryptosystem.
The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted) [8]. Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption [9] to e-mail privacy [10] and secure remote access [11]. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken [12] [13].

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher. Block ciphers can be used as stream ciphers.

3. Conclusions

In this paper we basically talked about the state-of-the-art cryptographic techniques. Although there are constant improvement of data security and information storage systems but still cryptography needs to be more agile and robust. Our future work includes cryptographic implementation in image processing and storage systems.

References

[1] http://en.wikipedia.org/wiki/Cryptography
[2] Ahmed Al-Vahed, Haddad Sahhavi, "An Overview of Modern Cryptography", *World Applied Programming, Vol (1), No (1), April 2011. 3-8*
[3] David Kahn, The Codebreakers, 1967, ISBN 0-684-83130-9.
[4] Oded Goldreich, Foundations of Cryptography, Volume 1: Basic Tools, Cambridge University Press, 2001, ISBN 0-521-79172-3
[5] "Cryptology (definition)". Merriam-Webster's Collegiate Dictionary (11th edition ed.). Merriam-Webster. http://www.merriam-webster.com/dictionary/cryptology. Retrieved 2008-02-01.
[6] http://en.wikipedia.org/wiki/Public-key_cryptography
[7] James Massey, Gurgen Khachatrian, Melsik Kuregian, "Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE), " Presented in First Open NESSIE Workshop, November, 2000.
[8] FIPS PUB 197: The official Advanced Encryption Standard.
[9] NCUA letter to credit unions, July 2004
[10] RFC 2440 - Open PGP Message Format
[11] SSH at windowsecurity.com by Pawel Golen, July 2004
[12] AJ Menezes, PC van Oorschot, and SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-8523-7.

[13] Bruce Schneier, Applied Cryptography, 2nd edition, Wiley, 1996, ISBN 0-471-11709-9.

Mohiuddin Ahmed has achieved Bachelor of Computer Science & Information Technology from Islamic University of Technology, OIC. Now working as a lecturer at Green University of Bangladesh in Computer Science & Engineering Department. Research Interest includes Human-Computer Interaction, Cloud Computing, Artificial Intelligence, Wireless Network, Computational Mathematics.

T. M. Shahriar Sazzad is a research student in Image Processing. He has completed MSc in Information Technology from UK. Interested areas include Image Processing, Cloud Computing and Artificial Intelligence.

Md. Elias Mollah is working as a lecturer of Computer Science & Engineering Department at Green University of Bangladesh. Research interest includes Computer Networking, Cryptography, Computational Algebra, Artificial Intelligence.