Analysis and Design of Cryptography Algorithms

Pratik A. Vanjara
Deptt. of CS & IT
Shree. M & N Virani Science
College, Rajkot, India

ABSTRACT

This paper analyzes the security of a recently-proposed signal encryption scheme based on Different Algorithms. A very critical weakness of this new signal encryption procedure is exploited in order to successfully recover the associated secret key.

Keywords

Cryptography, Security, Authentication.

1. CYRPTOGRAPHIC ALGORITHMS

Cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher messages in a cryptographic system. In simple terms, they're processes that protect data by making sure that unwanted people can't access it. These algorithms have a wide variety of uses, including ensuring secure and authenticated financial transactions.

Most cryptography algorithms involve the use of encryption, which allows two parties to communicate while preventing unauthorized third parties from understanding those communications. Encryption transforms human readable plaintext into something unreadable, also known as *ciphertext*. The encrypted data is then decrypted to restore it, making it understandable to the intended party. Both encryption and decryption operate based on algorithms.

There are many different types of cryptographic algorithms, though most of them fit into one of two classifications — symmetric and asymmetric. Some systems, however, use a hybrid of both classifications. Symmetric algorithms, also known as symmetric-key or shared-key algorithms, work by the use of a key known only to the two authorized parties. While these can be implemented in the form of block ciphers or stream ciphers, the same key is used for both encrypting and decrypting the message. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the most popular examples of symmetric cryptography algorithms.

Asymmetric cryptography algorithms rely on a pair of keys — a public key and a private key. The public key can be revealed, but, to protect the data, the private key must be concealed. Additionally, encryption and decryption of the data must be done by the associated private and public keys. For example, data encrypted by the private key must be decrypted by the public key, and vice versa. RSA is one of the most common examples of this algorithm.

Symmetric algorithms are usually much faster than asymmetric algorithms. This is largely related to the fact that only one key is required. The disadvantage of shared-key systems, however, is that both parties know the secret key. Additionally, since the algorithm used is the public domain, it is actually the key that controls access to the data. For these reasons, the keys must be safe-guarded and changed relatively frequently to ensure security.

2. TRADITIONAL VERSUS MODERN CRYPTOGRAPHY

Today's cryptography is vastly more complex than its predecessor. Unlike the original use of cryptography in its classical roots where it was implemented to conceal both diplomatic and military secrets from the enemy, the cryptography of today, even though it still has far-reaching military implications, has expanded its domain, and has been designed to provide a cost-effective means of securing and thus protecting large amounts of electronic data that is stored and communicated across corporate networks worldwide. Cryptography offers the means for protecting this data all the while preserving the privacy of critical personal financial, medical, and ecommerce data that might end up in the hands of those who shouldn't have access to it.

The task of cryptographers is to design algorithms that achieve some cryptographic goal and that have no property that a random algorithm would not have, to some extent. The task of cryptanalysts is to analyze those algorithms, and in particular to seek a structure in order to devise specific attacks (like key-recovery or collision search), or merely to distinguish them from ideal algorithms. When an attack is found, the needle in the haystack is discovered either by applying a previous attack strategy, or by employing some ad hoc trick, or with a new generic attack method.

There have been many advances in the area of modern cryptography that have emerged beginning in the 1970s as the development of strong encryption-based protocols and newly developed cryptographic applications began to appear on the scene. On January, 1977, the National Bureau of Standards (NBS) adopted a data encryption standard called the Data Encryption Standard (DES), which was a milestone in launching cryptography research and development into the modern age of computing technology. Moreover, cryptography found its way into the commercial arena when, on December, 1980, the same algorithm, DES, was adopted by the American National Standards Institute (ANSI). Following this milestone was yet another when a new concept was proposed to develop Public Key Cryptography (PKC), which is still undergoing research development today (Levy, 2001).

Cryptography is considered not only a part of the branch of mathematics, but also a branch of computer science. There are two forms of cryptosystems: symmetric and asymmetric. Symmetric cryptosystems involve the use of a single key known as the secret key to encrypt and decrypt data or messages. Asymmetric cryptosystems, on the other hand, use one key (the public key) to encrypt messages or data, and a second key (the secret key) to decipher or decrypt those messages or data. For this reason, asymmetric cryptosystems are also known as public key cryptosystems. The problem that symmetric cryptosystems have always faced is the lack of a secure means for the sharing of the secret key by the individuals who wish to secure their data or communications. Public key cryptosystems solve this problem through the use of cryptographic algorithms used to create the public key and the secret key, such as DES, which has already been mentioned, and a much stronger algorithm, RSA. The RSA algorithm is the most popular form of public key cryptosystem, which was developed by Ron Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology in 1977 (Robinson, 2008). The RSA algorithm involves the process of generating the public key by multiplying two very large (100 digits or more) randomly chosen prime numbers, and then, by randomly choosing another very large number, called the encryption key. The public key would then consist of both the encryption key and the product of those two primes. Ron Rivest then developed a simple formula by which someone who wanted to scramble a message could use that public key to do so. The plaintext would then be converted to ciphertext, which was transformed by an equation that included that large product. Lastly, using an algorithm developed through the work of the great mathematician, Euclid, Ron Rivest provided for a decryption key—one that could only be calculated by the use of the original two prime numbers. Using this encryption key would unravel the ciphertext and transform it back into its original plaintext. What makes the RSA algorithm strong is the mathematics that is involved. Ascertaining the original randomly chosen prime numbers and the large randomly chosen number (encryption key) that was used to form the product that encrypted the data in the first place is nearly impossible (Levy, 2001).

A very popular public key cryptosystem is known as Pretty Good Privacy (PGP), developed by Phil Zimmerman beginning in early 1991 (Levy, 2001). The strength of the keys that are created to encrypt and decrypt data or communications is a function of the length of those keys. Typically the longer the key, the stronger that key is. For example, a 56-bit key (consisting of 56 bits of data) would not be as strong as a 128-bit key. And, consequently, a 128-bit key would not be as strong as a 256- or 1024-bit key. Scholarly Literature

3. TRENDS IN RESEARCH

There is a prevailing myth that secrecy is good for security, and since cryptography is based on secrets, it may not be good for security in a practical sense (Schneier, 2004; Baker, 2005). The mathematics involved in good cryptography is very complex and often difficult to understand, but many software applications tend to hide the details from the user thus making cryptography a useful tool in providing network and data security (Robinson, 2008). Many companies are incorporating data encryption and data loss prevention plans, based on strong cryptographic techniques, into their network security strategic planning programs (Companies Integrate, 2006).

Cryptographic long-term security is needed but is often difficult to achieve. Cryptography serves as the foundation for most IT security solutions, which include: (1) Digital signatures that are used to verify the authenticity of updates for computer operating systems, such as Windows XP; (2) Personal banking, ecommerce, and other Web-based applications that rely heavily on Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for authentication and data security; and (3) The introduction of health cards that allow access to medical history, prescription history, and medical records in countries such as Germany, which contain the electronic health information of its citizens and which depend on digital signature and other encryption schemes for security and privacy of critical data (Perspectives for, 2006). There are product design criteria that designers can meet for implementing strong encryption protocols into software applications; however, strong public-key cryptography may prove too computationally expensive for small devices, and the alternative may be to incorporate cryptographic hardware into embedded designs (Robinson, 2008). Although cryptography and information security are multi-billion dollar industries, the economy of the world and the defense of almost every nation worldwide depend upon it and could not be carried out without it (Fagin, Baird, Humphries, & Schweitzer, 2008).

An individual’s identity in the digital world could be controlled by what is termed the federated identity management system consisting of software components and protocols that manage the identify of individuals throughout their identity lifecycle (Bhargav-Spantzel, Camenisch, Gross, & Sommer, 2007). With the rise in threats to sensitive data from outsiders, encryption is seen as a necessary tool in ensuring corporate networks and individuals’ information is as secure as possible (Toubba, 2006).

It is the intent of this review of the literature to look at what has been published regarding cryptography algorithms in recent years from the standpoint of network and data security and privacy, and to specifically address the role that cryptography plays in enabling this security.

Scholarly Literature

One can see the principal goal of cryptography as turning order into disorder, or, more formally, as simulating randomness: block ciphers should ideally be pseudorandom permutations (PRP), stream ciphers should ideally be some special kinds of pseudorandom generators (PRG), and hash functions should be pseudorandom functions (PRF). From a theoretical standpoint, however, it is not known whether simulating randomness is possible, but it is widely believed. Indeed, PRG’s exist if and only if one-way functions exist, and one-way functions are believed to exist.

One subfield of cryptography is concerned with the design of provably secure schemes and protocols. It is sometimes called modern cryptography, and opposed to the classical approach that builds on ad hoc constructions and on third-party cryptanalysis. In the provable security approach, one formally defines notions of security, and specifies a model used for conducting proofs. The most common model is the so-called standard model, which minimizes abstractions as “oracles”. Common assumptions are the hardness of factoring and discrete logarithm (and variants thereof), or that AES is a good PRP. Although it relies on unproved assumptions and contains a part of abstraction, the standard model is regarded as the most realistic one.

When assumptions in the standard model are insufficient to achieve (or to prove) security, one often resorts to the random oracle model (ROM). Formalized by Bellare and Rogaway, the ROM gives to parties access to one or several public random functions that typically accept as input bit strings of any finite length. Schemes proved secure in the ROM are generally significantly more efficient than schemes proved secure in the standard model. But this model is often treated with suspicion, especially since the exhibition of uninstantiable schemes proved secure in the ROM. Similar results were given by Black for the ideal cipher model, which was recently proved to be polynomially equivalent to the ROM.

Although it provides essential guidance in the design of real-world schemes, the provable security approach does not guarantee security in the physical world, for any model fails to capture all the possible attack channels. Perhaps more importantly, security proofs do not extend to the physical world because PRP's, PRF's, PRG's are in practice all instantiated with symmetric algorithms that are not proved secure (proved secure algorithms exist, but are highly inefficient), while random oracles have no physical existence. Thus, cryptographic schemes eventually rely on cryptanalysis for acquiring confidence in their security. In particular, the approach of focused public cryptanalysis through cryptography competitions has proved its effectiveness; for instance, most researchers are now comfortable with the assumption that AES is a good PRP.

Now that we have analyzed some of the research that has been conducted and reported in scholarly literature, let's switch our focus and review some of the non-scholarly literature that has been published on this topic as well.

Non-Scholarly Literature

As pointed out in Companies Integrate (2008) many corporations are beginning to realize that using cryptography to encrypt the PC or perimeter device is not an all-inclusive, effective means of protecting their essential data. Taking measures to prevent data loss is also needed. Additionally with the myriad ways of sharing data on corporate networks and the Internet that exist today, it is time to employ strong cryptography as a means of securing the data and to protect individuals' privacy (Harris, 2007).

Many IT professionals and information security professionals are beginning to realize the importance of remaining current in the area of security through the development of information technology safeguards and corporate policies that keep companies' information assets secure. Since there is a greater reliance on cryptography as the means of securing those assets more effectively, many of these professionals are turning to the non-profit organization known as the International Information Systems Security (ISC) Certification Consortium, which has certified more than 42,000 information security professionals in 110 countries (Pratt 2006). Many of these IS security professionals must now manage complex applications that involve advanced cryptosystems that help corporations comply with a growing list of federally- and state-mandated regulations that commission strict data security and privacy.

4. CONCLUSION

It compares and Design the Algorithms. It analyzes the role that cryptography has played and will play in the future relative to security. This review addresses cryptography around the central theme of the design algorithms for the security that it provides or should provide individuals, corporations, and others in the modern age of computing technology, networking, and Web-based ecommerce. By reviewing both scholarly and non-scholarly works, it is our objective to make a case that continuing research into the use of cryptography is paramount in preserving the future of electronic data security and privacy as well as the continuing development of algorithms that will permit the growth of security worldwide to be conducted over the world.

5. REFERENCES

[1] Kazumaro Aoki and Kazuhiro Kurokawa. A study on linear cryptanalysis of Multi2 (in Japanese). In The 1995 Symposium on Cryptography and Information Security, SCIS95,1995.

[2] Shor P 1994 Algorithms for Quantum Computation: Discrete Logarithms and Factoring in *Proc. 35th Ann. Symp. Found. Comp. Sci.* 124.

[3] Aharonov D, Jones V and Landau Z 2006 A polynomial quantum algorithm for approximating the Jones polynomial, in Proc. STOC2006 427

[4] Blackburn S R, Cid C and Mullan C 2009 Group theory in cryptography *eprint* arXiv:0906.5545v2

[5] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In Proc. of Crypto'89, number 435 in Lecture Notes in Computer Science, pages 307{315. Springer-Verlag,1990.

[6] Ran Canetti and Hugo Krawczyk. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In Birgit Pfitzmann, editor, *Advances in* Cryptology – EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, pages 453–474. Springer, 2001

[7] Generalized Key Delegation for Hierarchical Identity-Based Encryption-June 2007

[8] Data Encryption Standard Book

[9] Robust Encryption Michel Abdalla1 Mihir Bellare2 Gregory Neven3

[10] Post Quantum Cryptography from Mutant Prime Knots Annalisa Marzuoli and Giandomenico Palumbo

[11] Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness Michel Abdalla 1, Dario Catalano 2, Céline Chevalier 1, and David Pointcheval 1

[12] Threshold Cryptography Based on Asmuth-Bloom Secret Sharing? Kamer Kaya?? , Ali Ayd_n Sel_cuk, Zahir Tezcan

[13] Wildcarded Identity-Based Encryption?

[14] (Password) Authenticated Key Establishment: From 2-Party To Group Michel Abdalla1, Jens-Matthias Bohli2, Mar´ıa Isabel Gonz´alez Vasco3,and Rainer Steinwandt4

[15] an approach to enhance image encryption using blockbased transformation algorithm mohammad ali moh'd bani younes

[16] Cryptanalysis of a computer cryptography scheme based on a filter bank David Arroyo a,_, Chengqing Li b, Shujun Li c and Gonzalo Alvarez a

[17] Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm David Arroyo a,∗, Chengqing Li b, Shujun Li c, Gonzalo Alvarez a and Wolfgang A. Halang c

[18] a short survey on visual cryptography schemes from jim cai

[19] new randomized data hiding algorithm with encrypted secret message using modified generalized Vernam Cipher Method: RAN-SEC algorithm Rishav Ray, Jeeyan Sanyal2, Tripti Das3, Kaushik Goswami4, Sankar Das5, Asoke Nath6

[20] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm *Joyshree Nath A.K.Chaudhuri School of I.T*

y