Thesis

on

Cryptography

Submitted

by

Ms. Saakshi Agrawal

(171081024)

Under Supervision of

Mr. Pranav Nerurkar

Department of Computer Engineering & Information Technology

Veermata Jijabai Technological Institute, Mumbai - 400019

(Autonomous Institute Affiliated to University of Mumbai)

2018 - 2019

CERTIFICATE

This is to certify that, **Saakshi Agrawal (ID- 171081024)**, a student of **Bachelor Of Technology (Information Technology)** has completed the lab report held in Jan-Feb 2019 for working on latex to our satisfaction.

Mr.Pranav Nerurkar
Supervisor

Dr. V. B. Nikam
HOD of CE & IT

Date:
Place:

Declaration of the Student

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources.

I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea / data / fact / source in my submission.

I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Saakshi Agrawal
(Reg no : 171081024) Date: ________________

Acknowledgements

My sincere thanks goes to Dr. Dhiren Patel, Director of Veermata Jijabai Technological Institute, Mumbai who provided me an opportunity to work as a research scholar and gave me access to the laboratory and research facilities which helped me to conduct this research.

I would like to express my sincere gratitude to my co-supervisor Dr. M. M. Chandane and supervisor Dr. S. G. Bhirud for the continuous support of my Ph.D study and related research, for their patience, motivation, and immense knowledge. Their guidance helped me in all the time of research and writing of this report.

I thank our Head of the Department Dr. V. B. Nikam, for extending his invaluable support. I would also thank my institute and the department's faculty members without whom this research work would have been a distant reality.

I also extend my heartfelt thanks to my family and well wishers.

Date:

ABSTRACT

In the spirit of algebraic abstraction, this paper advocates the definition and use of higher levels of abstraction in cryptography (and beyond). If contrasted with the standard bottom-up approach to defining models of computation, algorithms, complexity, efficiency, and then security of cryptographic schemes, our approach is top-down and axiomatic, where lower abstraction levels inherit the definitions and theorems (e.g. a composition theorem) from the higher level, but the definition or concretization of low levels is not required for proving theorems at the higher levels. The goal is to strive for simpler definitions, higher generality of results, simpler proofs, improved elegance, possibly better didactic suitability, and to derive new insights from the abstract viewpoint.

In particular, we propose a general framework for defining and proving that a system satisfying an (abstract or ideal) specification is constructed from some systems satisfying certain (concrete or real) specifications. This puts the well-known “ideal-world real-world ” paradigm on a new theoretical foundation, applicable in various cryptographic settings. Existing frameworks for proving composable security can be explained as special cases of our framework, thereby allowing to distinguish between relevant and less relevant aspects of the underlying technical definitions and to prove a single common composition theorem. Some properties of our framework are as follows. It is independent of particular models of computation, communication,

Contents

Chapter 1

INTRODUCTION

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.[11] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.[2] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that probably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation.[12] Cryptography also plays a major role in digital rights management and copyright infringement of digital media.[5]

Chapter 2

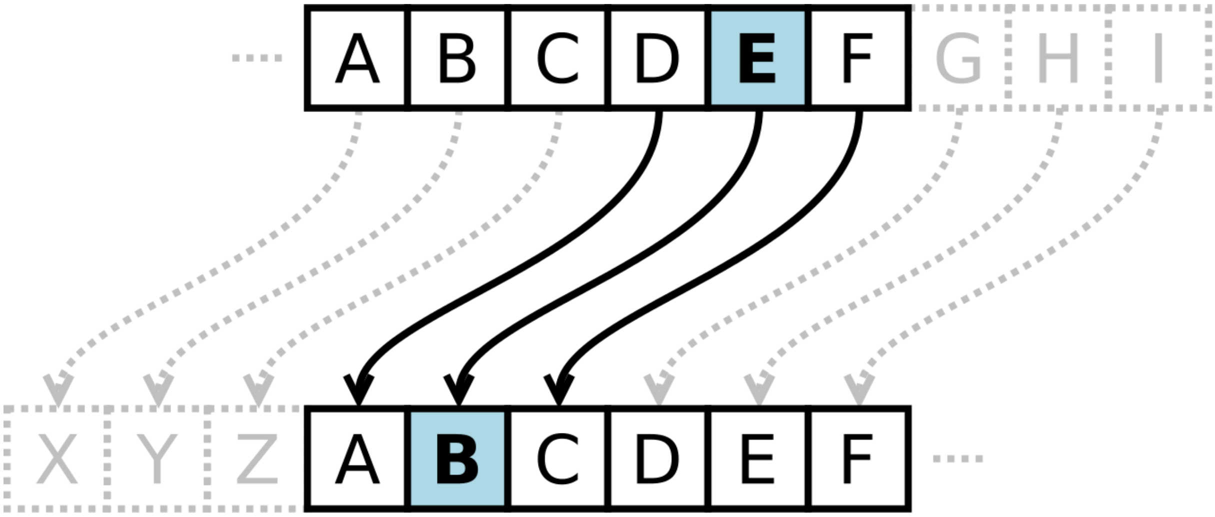
TERMINOLOGY

The first use of the term cryptograph (as opposed to cryptogram) dates back to the 19th century—it originated in The Gold-Bug, a novel by Edgar Allan Poe.[9]

Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext).[7] Decryption is the reverse, in other words, moving from the unintelligible ciphertext 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". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext. Formally, 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 both formally and in actual practice, 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. There are two kinds of cryptosystems: symmetric and asymmetric. In symmetric systems the same key (the secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication.[13] Examples of asymmetric systems include RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve

Cryptography). Symmetric models include the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard).



Alphabet shift ciphers are believed to have been used by Julius Caesar over 2,000 years ago.[2] This is an example with k=3. In other words, the letters in the alphabet are shifted three in one direction to encrypt and three in the other direction to decrypt.

Chapter 3

MODERN CRYPTOGRAPHY

Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics. There are very few cryptosystems that are proven to be unconditionally secure. The one-time pad is one, and was proven to be so by Claude Shannon. There are a few important algorithms that have been proven secure under certain assumptions. For example, the infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and some other systems, but even so proof of unbreakability is unavailable since the underlying mathematical problem remains open. In practice, these are widely used, and are believed unbreakable in practice by most competent observers. There are systems similar to RSA, such as one by Michael O. Rabin that are provably secure provided factoring [$n = pq$] is impossible; it is quite unusable in practice. The discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again, there are related, less practical systems that are provably secure relative to the solvability or insolvability discrete log problem.[4]

As well as being aware of cryptographic history, cryptographic algorithm and system designers must also sensibly consider probable future developments while working on their designs. For instance, continuous improvements in computer processing power have increased the scope of brute-force attacks, so when specifying key lengths, the required key lengths are similarly advancing. The potential effects of quantum computing are already being considered by some cryptographic system designers developing post-quantum cryptography; the announced imminence of small implementations of these machines may be making the need for preemptive caution rather more than merely speculative.

3.1 Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.[4]

logic diagram showing International Data Encryption Algorithm cypher process One round (out of 8.5) of the IDEA cipher, used in most versions of PGP and OpenPGP compatible software for time-efficient encryption of messages

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government. Despite its deprecation as an official standard, DES remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy[13] and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many, even some designed by capable practitioners, have been thoroughly broken, such as FEAL.[2]

3.2 Public-key cryptography

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. While Diffie and Hellman could not find such a system, they showed that public-key cryptography was indeed possible by presenting the Diffie–Hellman key exchange protocol, a solution that is now widely used in secure communications to allow two parties to secretly agree on a shared encryption key.[7]

Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.

3.3 Cryptanalysis

The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

It is a common misconception that every encryption method can be broken. In connection with his WWII work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message.[14] Most ciphers, apart from the one-time pad, can be broken with enough computational effort by brute force attack, but the amount of effort needed may be exponentially dependent on the key size, as compared to the effort needed to make use of the cipher. In such cases, effective security could be achieved if it is proven that the effort required (i.e., "work factor", in Shannon's terms) is beyond the ability of any adversary. This means it must be shown that no efficient method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no such proof has been found to date, the one-time-pad remains the only theoretically unbreakable cipher.

3.4 Cryptographic primitives

Much of the theoretical work in cryptography concerns cryptographic primitives—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called cryptosystems or cryptographic protocols, which guarantee one or more high-level security properties. Note however, that the distinction between cryptographic primitives and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

3.5 Cryptosystems

One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or cryptosystem. Cryptosystems (e.g., El-Gamal encryption) are designed to provide particular functionality (e.g., public key encryption) while guaranteeing certain security properties (e.g., chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. As the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems. In many cases, the cryptosystem's structure involves back and forth communication among two or more parties in space

Table 3.1: Cryptography Primitives

Services	**Encryption**	**Hash Function**	**MAC**	**Digital Sign**
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes

(e.g., between the sender of a secure message and its receiver) or across time (e.g., cryptographically protected backup data). Such cryptosystems are sometimes called cryptographic protocols.

Some widely known cryptosystems include RSA encryption, Schnorr signature, El-Gamal encryption, PGP, etc. More complex cryptosystems include electronic cash[1] systems, signcryption systems, etc. Some more 'theoretical'[clarification needed] cryptosystems include interactive proof systems,[14] (like zero-knowledge proofs),[6] systems for secret sharing, etc.

Chapter 4

LEGAL ISSUES

4.1 Prohibitions

In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France significantly restricted the use of cryptography domestically, though it has since relaxed many of these rules. In China and Iran, a license is still required to use cryptography. Many countries have tight restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Singapore, Tunisia, and Vietnam.[10] In the United States, cryptography is legal for domestic use, but there has been much conflict over legal issues related to cryptography. One particularly important issue has been the export of cryptography and cryptographic software and hardware. Probably because of the importance of cryptanalysis in World War II and an expectation that cryptography would continue to be important for national security, many Western governments have, at some point, strictly regulated export of cryptography. After World War II, it was illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was designated as auxiliary military equipment and put on the United States Munitions List.[10] Until the development of the personal computer, asymmetric key algorithms (i.e., public key techniques), and the Internet, this was not especially problematic. However, as the Internet grew and computers became more widely available, high-quality encryption techniques became well known around the globe.

4.2 Export controls

In the 1990s, there were several challenges to US export regulation of cryptography. After the source code for Philip Zimmermann's Pretty Good Privacy (PGP) encryption program found its way onto the Internet in June 1991, a complaint by RSA Security (then called RSA Data Security, Inc.) resulted in a lengthy criminal investigation of Zimmermann by the US Customs Service and the FBI, though no charges were ever filed.[14] Daniel J. Bernstein, then a graduate student at UC Berkeley, brought a lawsuit against the US government challenging some aspects of the restrictions based on free speech grounds. The 1995 case Bernstein v. United States ultimately resulted in a 1999 decision that printed source code for cryptographic algorithms and systems was protected as free speech by the United States Constitution.[1]

In 1996, thirty-nine countries signed the Wassenaar Arrangement, an arms control treaty that deals with the export of arms and "dual-use" technologies such as cryptography. The treaty stipulated that the use of cryptography with short key-lengths (56-bit for symmetric encryption, 512-bit for RSA) would no longer be export-controlled. Cryptography exports from the US became less strictly regulated as a consequence of a major relaxation in 2000;[10] there are no longer very many restrictions on key sizes in US-exported mass-market software. Since this relaxation in US export restrictions, and because most personal computers connected to the Internet include US-sourced web browsers such as Firefox or Internet Explorer, almost every Internet user worldwide has potential access to quality cryptography via their browsers (e.g., via Transport Layer Security). The Mozilla Thunderbird and Microsoft Outlook E-mail client programs similarly can transmit and receive emails via TLS, and can send and receive email encrypted with S/MIME. Many Internet users don't realize that their basic application software contains such extensive cryptosystems.

4.3 NSA involvement

Another contentious issue connected to cryptography in the United States is the influence of the National Security Agency on cipher development and policy.[15] The NSA was involved with the design of DES during its development at IBM and its consideration by the National Bureau of

Standards as a possible Federal Standard for cryptography.[3] DES was designed to be resistant to differential cryptanalysis, a powerful and general cryptanalytic technique known to the NSA and IBM, that became publicly known only when it was rediscovered in the late 1980s. According to Steven Levy, IBM discovered differential cryptanalysis[8] but kept the technique secret at the NSA's request. The technique became publicly known only when Biham and Shamir re-discovered and announced it some years later. The entire affair illustrates the difficulty of determining what resources and knowledge an attacker might actually have.

Another instance of the NSA's involvement was the 1993 Clipper chip affair, an encryption microchip intended to be part of the Capstone cryptography-control initiative. Clipper was widely criticized by cryptographers for two reasons. The cipher algorithm was then classified. The classified cipher caused concerns that the NSA had deliberately made the cipher weak in order to assist its intelligence efforts.

Bibliography

[1] László Babai. *Trading group theory for randomness. Proceedings of the Seventeenth Annual Symposium on the Theory of Computing.* 1985.

[2] Norman Biggs. Codes: An introduction to information communication and cryptography. 2008.

[3] Bruce. *Data Encryption.* 2000.

[4] Martin Diffie, Whitfield; Hellman.

[5] Cory Doctorow. *Digg users revolt over AACS key.* 2007.

[6] S.; Rackoff C. Goldwasser, S.; Micali. *The Knowledge Complexity of Interactive Proof Systems.* 1989.

[7] David Kahn. *The Codebreakers.* 1967.

[8] Steven Levy. *Crypto.* 2001.

[9] Robert; Jones Henry Stuart Liddell, Henry George; Scott. Cryptography. 1984.

[10] Martin. Cryptographic policies. 2015.

[11] Ronald L. Rivest. Cryptography. 1990.

[12] Robert. *UK Data Encryption Disclosure Law Takes Effect*. 2005.

[13] Sam. An introduction to modern cryptosystems.

[14] Warren Shannon, Claude; Weaver. 1963, title=.

[15] Steve. *internet secrets*. 2015.