Cryptography

Saakshi Agrawal
Guided by Mr. Pranav Nerurkar
Dept of Computer Engineering and IT
Veermata Jijabai Technological Institute
Maharashtra, Mumbai 400019

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.**

I. INTRODUCTION

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.[1] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages;[2] 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.[3] 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 poweran example is the one-time padbut 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.[4] Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

II. TERMINOLOGY

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

Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext).[5] 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. 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).[6]

In colloquial use, the term ”code” is often used to mean any method of encryption or concealment of meaning. However, in cryptography, code has a more specific meaning. It means the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, ”wallaby” replaces ”attack at dawn”).

Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations.

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. English is more flexible than several other languages in which cryptology (done by cryptologists) is always used in the second sense above. RFC 2828 advises that steganography is sometimes included in cryptology.

The study of characteristics of languages that have some application in cryptography or cryptology (e.g. frequency data, letter combinations, universal patterns, etc.) is called cryptolinguistics.

III. Modern cryptography

- Symmetric-key cryptography Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys.[7] The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[8] This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).[9]
- Public-key cryptography Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.[10] In such a system, any person can encrypt a message using the receiver’s public key, but that encrypted message can only be decrypted with the receiver’s private key.
- Cryptanalysis Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it; cryptanalysts also target secure hashing, digital signatures and other cryptographic algorithms. While the objective of cryptanalysis is to find weaknesses in or otherwise defeat cryptographic algorithms, cryptanalysts’ research results are used by cryptographers to improve and strengthen or replace flawed algorithms. Both cryptanalysis, which focuses on deciphering encrypted data, and cryptography, which focuses on creating and improving encryption ciphers and other algorithms, are aspects of cryptology, the mathematical study of codes, ciphers and related algorithms.
- Cryptographic primitives Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security systems. These routines include, but are not limited to, one-way hash functions and encryption functions.When creating cryptographic systems, designers use cryptographic primitives as their most basic building blocks. Because of this, cryptographic primitives are designed to do one very specific task in a highly reliable fashion. Since cryptographic primitives are used as building blocks, they must be very reliable, i.e. perform according to their specification.
- Cryptosystems In cryptography, a cryptosystem is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality (encryption).[11]
  Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. The term cipher (sometimes cypher) is often used to refer to a pair of algorithms, one for encryption and one for decryption. Therefore, the term cryptosystem is most often used when the key generation algorithm is important. For this reason, the term cryptosystem

is commonly used to refer to public key techniques; however both ”cipher” and ”cryptosystem” are used for symmetric key techniques.

IV. Conclusion

Security in the Internet is improving. The increasing use of the Internet for commerce is improving the deployed technology to protect the financial transactions. Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread. Control over routing remains the basic tool for controlling access to streams. Implementing particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for communications. However, cryptography requires the safe implementation of complex mathematical equations and protocols, and there are always worries about bad implementations. A further worry is that users are integral to securing communications, since they must provide appropriate keys. As the founders of First Virtual point out a safe application of cryptographic technology will pay close attention to how public keys are associated with user identities, how stolen keys are detected and revoked and how long a stolen key is useful to a criminal. Cryptography may be groovy technology, but since security is a human issue, cryptography is only as good as the practices of the people who use it. Users leave keys lying around, choose easily remembered keys, don’t change keys for years. The complexity of cryptography effectively puts it outside the understanding of most people and so motivation for the practices of cryptographic security is not available.

References

[1] Ronald L. Rivest. Cryptography. 19(1-12):888–896, 1990.

[2] Phillip Bellare, Mihir; Rogaway. Introduction to modern cryptography. 10:118–173, 2005.

[3] Codes: An introduction to information communication and cryptography.

[4] The undercover war on your internet secrets: How online surveillance cracked our trust in the web. 2015.

[5] David Kahn. The codebreakers. 1967.

[6] Quantum cryptography: An emerging technology in network security,’ year=.

[7] Zaid Kartit. *Applying Encryption Algorithms for Data Security in Cloud Storage*. 2016.

[8] Hans Knebl Delfs. *Symmetric-key encryption*. 2007.

[9] *Finite fields and applications*. 2007.

[10] *Cryptography and Network Security: Principles and Practice*. 1990.

[11] P. van; Vanstone Menezes, A.; Oorschot. *Handbook of Applied Cryptography*. 2005.