International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

Review paper on cryptography

Neelima Saini & Sunita Mandal
Dronacharay college of engineering , Gurgaon
Neelimasaini1994@gmail.com, coolsunita mandal@gmail.com

1 Introduction

Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.

Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". People who study and develop cryptography are called**cryptographers**. The study of how to *circumvent* the use of cryptography for unintended recipients is called **cryptanalysis**, or codebreaking. Cryptography and cryptanalysis are sometimes grouped together under the **umbrella** term cryptology, encompassing the entire subject. In practice, "cryptography" is also often used to refer to the field as a whole, especially as an applied science.

Cryptography is an interdisciplinary subject, drawing from several fields. Before the time of computers, it was closely related to linguistics. Nowadays the emphasis has shifted, and cryptography makes extensive use of technical areas of mathematics, especially those areas collectively known as discrete mathematics. This includes topics from number theory, information theory, computational complexity, statistics and combinatorics. It is also a branch of engineering, but an unusual one as it must deal with active, intelligent and malevolent opposition.

An example of the sub-fields of cryptography is **steganography** — the study of hiding the very *existence* of a message, and not necessarily the *contents* of the message itself (for example, microdots, or invisible ink) — and **traffic analysis**, which is the analysis of patterns of communication in order to learn secret information.

When information is transformed from a *useful form* of understanding to an *opaque form* of understanding, this is called **encryption**. When the information is reverted back into a useful form, it is called **decryption**. Intended recipients or authorized use of the information is determined by whether the user has a certain piece of secret knowledge. *Only* users with the secret knowledge can transform the opaque information back into its useful form. The secret knowledge is commonly called the **key**, though the secret knowledge may include the *entire process* or algorithm that is used in the encryption/decryption. The information in its useful form is called **plaintext** (or cleartext); in its encrypted form it is called **ciphertext**. The algorithm used for encryption and decryption is called a **cipher** (or cypher).

2 common goals in cryptography

In essence, cryptography concerns four main goals. They are:

1. message **confidentiality** (or privacy): Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information.
2. message **integrity**: The recipient should be able to determine if the message has been altered.
3. sender **authentication**: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled (or combinations) so to validate claims from emitter or to validated the recipient expectations.
4. sender **non-repudiation**: The emitter should not be able to deny sending the message.

Not all cryptographic systems achieve all of the above goals. Some applications of cryptography have *different* goals; for example some situations require **repudiation** where a participant can plausibly deny that they are a sender or receiver of a message, or extend this goals to include variations like:

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

1. message **access control**: Who are the valid recipients of the message.
2. message **availability**: By providing means to limit the validity of the message, channel, emitter or recipient in time or space.

3Classical Cryptography

The earliest known use of cryptography is found in non-standard hieroglyphs carved into monuments from Egypt's Old Kingdom (ca 4500 years ago). These are not thought to be serious attempts at secret communications, however, but rather to have been attempts at mystery, intrigue, or even amusement for literate onlookers. These are examples of still another use of cryptography, or of something that looks (impressively if misleadingly) like it. Later, Hebrew scholars made use of simple Substitution ciphers (such as the Atbash cipher) beginning perhaps around 500 to 600 BCE. Cryptography has a long tradition in religious writing likely to offend the dominant culture or political authorities. Perhaps the most famous is the 'Number of the Beast' from the book of Revelations in the Christian New Testament. '666' is almost certainly a cryptographic (i.e., encrypted) way of concealing a dangerous reference; many scholars believe it's a concealed reference to the Roman Empire, or the Emperor Nero, (and so to Roman policies of persecution of Christians) that would have been understood by the initiated (who 'had the codebook'), and yet be safe (or at least somewhat deniable and so less dangerous) if it came to the attention of the authorities. At least for orthodox Christian writing, the need for such concealment ended with Constantine's conversion and the adoption of Christianity as the official religion of the Empire.

The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cypher claimed to have been used by the Spartan military). Herodutus tells us of secret messages physically concealed beneath wax on wooden tablets or as a tattoo on a slave's head concealed by regrown hair (these are not properly examples of cryptography per se; see secret writing). The Romans certainly did (e.g., the Caesar cipher and its variations). There is ancient mention of a book about Roman military cryptography (especially Julius Caesar's); it has been, unfortunately, lost.

In India, cryptography was apparently well known. It is recommended in the Kama Sutra as a technique by which lovers can communicate without being discovered. This may imply that cryptanalytic techniques were less than well developed in India ca 500 CE.

Cryptography became (secretly) important still later as a consequence of political competition and religious analysis. For instance, in Europe during and after the Renaissance, citizens of the various Italian states, including the Papacy, were responsible for substantial improvements in cryptographic practice (e.g., polyalphabetic ciphers invented by Leon Albertica 1465). And in the Arab world, religiously motivated textual analysis of the Koran led to the invention of the frequency analysis technique for breaking monoalphabetic substitution cyphers sometime around 1000 CE.

Cryptography, cryptanalysis, and secret agent betrayal featured in the Babington plot during the reign of Queen Elizabeth I which led to the execution of Mary, Queen of Scots. And an encrypted message from the time of the Man in the Iron Mask (decrypted around 1900 by Étienne Bazeries) has shed some, regrettably non-definitive, light on the identity of that legendary, and unfortunate, prisoner. Cryptography, and its misuse, was involved in the plotting which led to the execution of Mata Hari and even more reprehensibly, if possible, in the travesty which led to Dreyfus' conviction and imprisonment, both in the early 20th century. Fortunately, cryptographers were also involved in setting Dreyfus free; Mata Hari, in contrast, was shot.

Mathematical cryptography leapt ahead (also secretly) after World War I. Marian Rejewski, in Poland, attacked and 'broke' the early German Army Enigma system (an electromechanical rotor cypher machine) using theoretical mathematics in 1932. The break continued up to '39, when changes in the way the German Army's Enigma machines were used required more resources than the Poles could deploy. His work was extended by Alan Turing, Gordon Welchman, and others at Bletchley Park beginning in 1939, leading to sustained breaks into several other of the Enigma variants and the assorted networks for which they were used. US Navy cryptographers (with cooperation from British and Dutch cryptographers after 1940) broke into several Japanese Navy crypto systems. The break into one of them famously led to the US victory in the Battle of Midway. A US Army group, the SIS, managed to break the highest security Japanese diplomatic cipher system (an electromechanical 'stepping switch' machine called Purple by the Americans) even before WWII began. The Americans referred to the intelligence resulting from cryptanalysis, perhaps especially that from the Purple machine, as 'Magic'.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

The British eventually settled on 'Ultra' for intelligence resulting from cryptanalysis, particularly that from message traffic enciphered by the various Enigmas. An earlier British term for Ultra had been 'Boniface'.

4 Modern Cryptography

The era of modern cryptography really begins with Claude Shannon, arguably the father of mathematical cryptography. In 1949 he published the paper Communication Theory of Secrecy Systems in the Bell System Technical Journal, and a little later the book *Mathematical Theory of Communication* with Warren Weaver. These, in addition to his other works on information and communication theory established a solid theoretical basis for cryptography and for cryptanalysis. And with that, cryptography more or less disappeared into secret government communications organizations such as the NSA. Very little work was again made public until the mid '70s, when everything changed.

1969 saw two major public (i.e., non-secret) advances. First was the DES (Data Encryption Standard) submitted by IBM, at the invitation of the National Bureau of Standards (now NIST), in an effort to develop secure electronic communication facilities for businesses such as banks and other large financial organizations. After 'advice' and modification by the NSA, it was adopted and published as a FIPS Publication (Federal Information Processing Standard) in 1977 (currently at FIPS 46-3). It has been made effectively obsolete by the adoption in 2001 of the Advanced Encryption Standard, also a NIST competition, as FIPS 197. DES was the first publicly accessible cypher algorithm to be 'blessed' by a national crypto agency such as NSA. The release of its design details by NBS stimulated an explosion of public and academic interest in cryptography. DES, and more secure variants of it (such as 3DES or TDES; see FIPS 46-3), are still used today, although DES was officially supplanted by AES (Advanced Encryption Standard) in 2001 when NIST announced the selection of Rijndael, by two Belgian cryptographers. DES remains in wide use nonetheless, having been incorporated into many national and organizational standards. However, its 56-bit key-size has been shown to be insufficient to guard against brute-force attacks (one such attack, undertaken by cyber civil-rights group The Electronic Frontier Foundation, succeeded in 56 hours -- the story is in *Cracking DES*, published by O'Reilly and Associates). As a result, use of straight DES encryption is now without doubt insecure for use in new crypto system designs, and messages protected by older crypto systems using DES should also be regarded as insecure. The DES key size (56-bits) was thought to be too small by some even in 1976, perhaps most publicly Whitfield Diffie. There was suspicion that government organizations even then had sufficient computing power to break DES messages and that there may be a back door due to the lack of randomness in the 'S' boxes.

Second was the publication of the paper New Directions in Cryptography by Whitfield Diffie and Martin Hellman. This paper introduced a radically new method of distributing cryptographic keys, which went far toward solving one of the fundamental problems of cryptography, key distribution. It has become known as Diffie-Hellman key exchange. The article also stimulated the almost immediate public development of a new class of enciphering algorithms, the asymmetric key algorithms.

Prior to that time, all useful modern encryption algorithms had been symmetric key algorithms, in which the same cryptographic key is used with the underlying algorithm by both the sender and the recipient who must both keep it secret. All of the electromechanical machines used in WWII were of this logical class, as were the Caesar and Atbash cyphers and essentially all cypher and code systems throughout history. The 'key' for a code is, of course, the codebook, which must likewise be distributed and kept secret.

Of necessity, the key in every such system had to be exchanged between the communicating parties in some secure way prior to any use of the system (the term usually used is 'via a secure channel') such as a trustworthy courier with a briefcase handcuffed to a wrist, or face-to-face contact, or a loyal carrier pigeon. This requirement rapidly becomes unmanageable when the number of participants increases beyond some (very!) small number, or when (really) secure channels aren't available for key exchange, or when, as is sensible crypto practice keys are changed frequently. In particular, a separate key is required for each communicating pair if no third party is to be able to decrypt their messages. A system of this kind is also known as a private key, secret key, or conventional key cryptosystem. D-H key exchange (and succeeding improvements) made operation of these systems much easier, and more secure, than had ever been possible before.

In contrast, with asymmetric key encryption, there is a pair of mathematically related keys for the algorithm, one of which is used for encryption and the other for decryption. Some, but not all, of these algorithms have the additional property that one of the keys may be made public since the other cannot be (by any currently known method) deduced from the 'public' key. The other key in these systems is kept secret and is usually called, somewhat confusingly, the 'private' key. An algorithm of this kind is known as a public key / private key algorithm, although the term asymmetric key cryptography is preferred by those who wish to avoid the ambiguity of using that term for all such algorithms, and to stress that there are two distinct keys with different secrecy requirements.

As a result, for those using such algorithms, only one key pair is now needed per recipient (regardless of the number of senders) as possession of a recipient's public key (by anyone whomsoever) does not compromise the 'security' of messages so long as the corresponding private key is not known to any attacker (effectively, this means not known to anyone except the recipient). This unanticipated, and quite surprising, property of some of these algorithms made possible, and made practical, widespread deployment of high quality crypto systems which could be used by anyone at all. Which in turn gave government crypto organizations worldwide a severe case of heartburn; for the first time ever, those outside that *fraternity* had access to cryptography that wasn't readily breakable by the 'snooper' side of those organizations. Considerable controversy, and conflict, began immediately. It has not yet subsided. In the US, for example, exporting *strong* cryptography remains illegal; cryptographic methods and techniques are classified as munitions. Until 2001 'strong' crypto was defined as anything using keys longer than 40 bits -- the definition was relaxed thereafter. (See S Levy's *Crypto* for a journalistic account of the policy controversy in the US).

5 Using Cryptosystems

- Applying Cryptography
- Digital Signatures
- Database protection
- E-Cash
- E-Voting
- DRM
- Biometrics
- Anonymity

6 Attacks

1. Brute-Force Attack
2. Frequency Analysis
3. Index of Coincidence
4. Linear Cryptanalysis
5. Differential Cryptanalysis
6. Meet in the Middle Attack
7. Man-in-the-middle attack

7 References

[1.] Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). *A Greek-English Lexicon*. Oxford University Press.

[2.] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. *Handbook of Theoretical Computer Science* **1**. Elsevier.

[3.] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. p. 10.

[4.] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. *Handbook of Applied Cryptography*. ISBN 0-8493-8523-7.

[5.] *Crypto Law Survey*. February 2013. Retrieved 26 March2015.

[6.] "UK Data Encryption Disclosure Law Takes Effect". *PC World*. 1 October 2007. Retrieved 26 March 2015.

[7.] Doctorow, Cory (2 May 2007). "Digg users revolt over AACS key". *Boing Boing*. Retrieved 26 March 2015.

[8.] Kahn, David (1967). *The Codebreakers*. ISBN 0-684-83130-9.

[9.] OdedGoldreich, *Foundations of Cryptography, Volume 1: Basic Tools*, Cambridge University Press, 2001, ISBN 0-521-79172-3

[10.] "Cryptology (definition)". *Merriam-Webster's Collegiate Dictionary* (11th ed.). Merriam-Webster. Retrieved 26 March 2015.

[11.] "RFC 2828 - Internet Security Glossary". *Internet Engineering Task Force*. May 2000. Retrieved 26 March 2015.

[12.] ÏAshchenko, V. V. (2002). *Cryptography: an introduction*. AMS Bookstore. p. 6. ISBN 0-8218-2986-6.

[13.] ^ Jump up to:[a] [b] Singh, Simon (2000). *The Code Book*. New York: Anchor Books. pp. 14–20.ISBN 9780385495325.

[14.] Al-Kadi, Ibrahim A. (April 1992). "The origins of cryptology: The Arab contributions".*Cryptologia* **16** (2): 97–126.

[15.] Schrödel, Tobias (October 2008). "Breaking Short Vigenère Ciphers". *Cryptologia* **32** (4): 334–337. doi:10.1080/01611190802336097.

[16.] Hakim, Joy (1995). *A History of US: War, Peace and all that Jazz*. New York: Oxford University Press. ISBN 0-19-509514-6.

[17.] Gannon, James (2001). *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*. Washington, D.C.: Brassey's. ISBN 1-57488-367-4.

[18.] Diffie, Whitfield; Hellman, Martin (November 1976). "New Directions in Cryptography" (PDF). *IEEE Transactions on Information Theory*. IT-22: 644–654.

[19.] Blaze, Matt; Diffie, Whitefield; Rivest, Ronald L.; Schneier, Bruce; Shimomura, Tsutomu; Thompson, Eric; Wiener, Michael (January 1996). "Minimal key lengths for symmetric ciphers to provide adequate commercial security". Fortify. Retrieved 26 March 2015.

[20.] "FIPS PUB 197: The official Advanced Encryption Standard" (PDF). *Computer Security Resource Center*. National Institute of Standards and Technology. Retrieved 26 March2015.

[21.] "NCUA letter to credit unions" (PDF). *National Credit Union Administration*. July 2004. Retrieved 26 March 2015.

[22.] "RFC 2440 - Open PGP Message Format". *Internet Engineering Task Force*. November 1998. Retrieved 26 March 2015.

[23.] Golen, Pawel (19 July 2002). "SSH". *WindowSecurity*. Retrieved 26 March 2015.

[24.] Schneier, Bruce (1996). *Applied Cryptography* (2nd ed.). Wiley. ISBN 0-471-11709-9.

[25.] "Notices". *Federal Register* **72** (212). 2 November 2007. Archived 28 February 2008 at the Wayback Machine

[26.] "NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition". *Tech Beat*.National Institute of Standards and Technology. October 2, 2012. Retrieved 26 March2015.

[27.] Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multi-user cryptographic techniques".*AFIPS Proceedings* **45**: 109–112.

[28.] Ralph Merkle was working on similar ideas at the time and encountered publication delays, and Hellman has suggested that the term used should be Diffie–Hellman–Merkleaysmmetric key cryptography.

[29.] Kahn, David (Fall 1979). "Cryptology Goes Public". *Foreign Affairs* **58** (1): 153.

[30.] Rivest, Ronald L.; Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM* (Association for Computing Machinery) **21** (2): 120–126.
Archived November 16, 2001 at the Wayback Machine
Previously released as an MIT "Technical Memo" in April 1977, and published in Martin Gardner's *Scientific American* Mathematical recreations column