History of Cryptography

AN EASY TO UNDERSTAND HISTORY OF CRYPTOGRAPHY

Contents

1. Introduction

Encryption and related technologies are widely and frequently used as a means of ensuring that information is secure, and their importance has been growing with the increasingly widespread utilization of the Internet.

The use of encryption can be traced to as far back as about 3000 B.C., during the Babylonian Era. Encryption technologies evolved as they were used in military and political settings, but as a result of the recent widespread use of the Internet and the dramatic increase in the amount of information people come into contact in their daily lives, the settings in which encryption technologies are applied and implemented have increased, and they are now used all around us in our daily lives.

The history of encryption is the history of “the contest of wits” between encryption developers and encryption code breakers. Each time a new encryption algorithm is created, it has been decrypted, and that in turn has led to the creation of a new encryption algorithm, and cycles of algorithm creation and decryption have been repeated to this day.

This white paper presents a brief history of cryptography and how encryption-related technologies have evolved and will continue to evolve as well as the measures Internet users should consider when implementing modern encryptions.

2. Classical Encryptions (Ancient Times)

Hieroglyphics (pictograms used in ancient Egypt) inscribed on a stele in about 3000 B.C. are considered the oldest surviving example of encryption. Hieroglyphics were long considered impossible to ever read, but the discovery and study of the Rosetta Stone in the 19th century was the catalyst that made it possible to read hieroglyphics.

The “scytale cipher” was a form of encryption used in the city state of Sparta in ancient Greece around the 6th century B.C. It involved the use of a cylinder of a certain diameter around which a parchment strip was wrapped, and the text was written on the parchment strip along the long axis of the cylinder. The method of encryption was designed so that the recipient would be able to read it by wrapping the parchment strip around a cylinder of the same diameter.

Encryption methods like the “scytale cipher” that rely on rearranging the sequence in which characters are read are referred to as “transposition ciphers”.

The Caesar cipher, which appeared in the 1st century B.C., was so named because it was frequently used by Julius Caesar, and it is a particularly prominent method of encryption among the great number of encryption methods that emerged during the long history of encryption.

The Caesar cipher method of encryption involves replacing each of the letters of the alphabet in the original text by a letter located a set number of places further down the sequence of the letters in the alphabet of the language. The sender and receiver agree in advance to replace each letter of the alphabet in the text by a letter that is, for example, three letters further down in their alphabet.

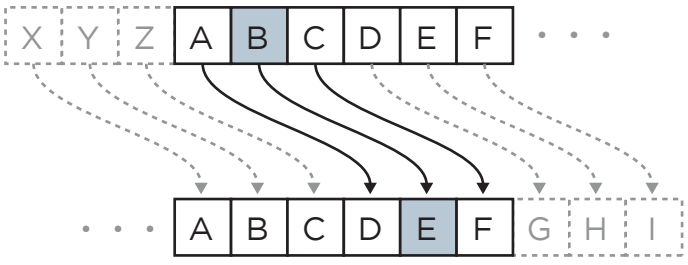

Figure 1

Since the Caesar cipher involved the shifting of characters, it is sometimes referred to as a “shift cipher”. If the alphabet consists of 26 letters, texts that have been encrypted by the Caesar cipher can be decrypted by trying 26 patterns. However, instead of simply shifting the characters by a fixed number of places in the alphabet, the sequence can be randomly rearranged, thereby significantly increasing the number of possible patterns (in the example of a 26-letter alphabet: 26 x 25 x 24 x …. = 400,000,000,000,000,000,000,000,000 patterns!) and making decryption dramatically more difficult.

Plain text characters (text that has not been encrypted)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption characters	SMKRATNGQJUDZLPVYOCWIBXFEH

An encryption method that involves rearranging the sequence of characters according to a specific rule such as that shown above is referred to as a “substitution cipher”. Substitution ciphers are a well-known encryption method, and they are the most commonly used encryption method in the history of encryption. The modern encryption machine called “Enigma” described below made it possible to apply the substitution cipher method with a higher level of sophistication.

The method of analysis that uses a reverse technique that takes advantage of the fact that only one letter can be substituted for each letter of the alphabet to decrypt “simple substitution ciphers” that depend on the letter substitution rule, e.g., the Caesar cipher, is known as “frequency analysis”.

Frequency analysis uses the frequency of letters (e.g. The English alphabet has common frequency characteristics for letters listed below) to speculate unencrypted characters and identify the original text:

- The letter “e” is the most frequently used letter. (Figure 2)
- The letter “u” almost always follows the letter “q”.
- The words “any”, “and”, “the”, “are”, “of”, “if”, “is”, “it”, and “in” are very common.

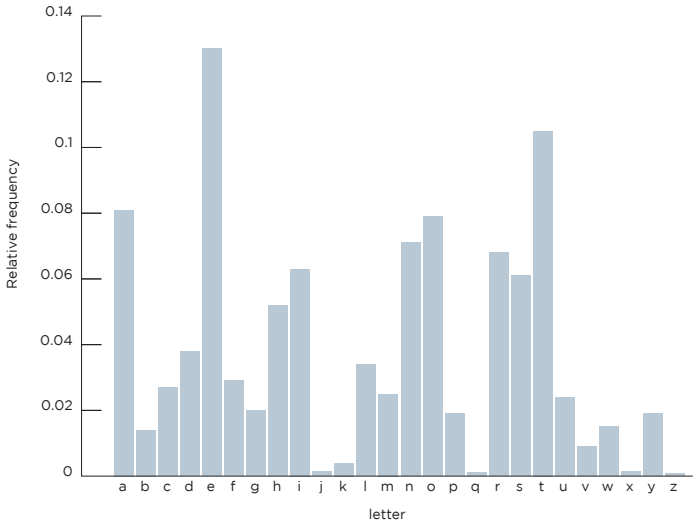

Figure 2

All of the encryption methods described above, including the substitution cipher and transposition cipher, consist of an “encryption algorithm” and a “key”. The encryption algorithm refers to the rules used for encrypting and decrypting text.

Encryption algorithms refer to the rule for encryption, for example, by shifting characters in a substitution ciphers, or using a cylinder to wrap a parchment strip around and write the message in the transposition cipher. The key refers to the number of places the characters are shifted in substitution ciphers and the diameter of the cylinder used for transposition ciphers. Since shifting characters by five places in the Caesar cipher is different from shifting them by four places, it means using different “keys”.

3. Classical Encryptions (Middle Ages)

Crytpography became more popular during the Middle Ages as encryption technologies became increasingly sophisticated based on the knowledge acquired during efforts to decrypt classical encryptions and the invention of new encryptions. The increased diplomatic activity during this time led to an increase in need to convey confidential information, which led to the frequent use of encryption.

The Cipher of Mary Queen of Scots

A weakness of the "simple substitution ciphers", typified by the Caesar cipher, was that only one encryption character could be assigned to each letter of the alphabet. A well-known example of decrypting in the 16th century that took advantage of this weakness was the decrypting of the cipher used by Mary Queen of Scots to communicate with her collaborators. The contents of those messages led to her being found guilty and executed for conspiring to assassinate Queen Elizabeth I of England.

The cipher Mary used was known as a "nomenclator cipher", and it included codes for replacing phrases in addition to replacing letters of the alphabet. These "codes" were listed in a "code book", i.e., the "key" to the cipher, that was in the possession of both senders and recipients, and it made decrypting the cipher more difficult.

Vigenère Ciphers

Simple substitution ciphers, which involve a pattern of replacing each character, like the one used by Mary Queen of Scots, eventually became decrypted. Moreover, the "nomenclator" used by Mary Queen of Scots involved the preparation of an enormous code book and providing a code book to each cipher user, which presented difficulties. The issue of "receiving and providing a key" has been a problem for users for advanced encryption technologies in the modern era as well as for users in the Middle Ages.

Early in the 15th century, Leon Battista Alberti devised the archetype for "polyalphabetic substitution" ciphers. They involve the use of two or more sets of encryption alphabets and have widely and frequently been used for decades. Because Blaise de Vigenère invented a strong final form of a polyalphabetic substitution cipher, such ciphers have been known as Vigenère ciphers since the 16th century.

Vigenère ciphers involve the use of a chart, known as the Vigenère Square (Figure 3). For example, if the key "OLYMPIC" is used to encrypt "GOLDMEDALIST", the letters in the original text refer to the characters listed across the top of the table and the letters in the key refer to the characters on the left side of the table, thereby finding the encrypted message at their intersections.

Plain text	GOLDMEDALIST
Key	OLYMPICOLYMP
Encrypted message	UZJPBMFOWGEI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 3

Since the messages encrypted with a Vigenère cipher are completely different depending on the keys, even if a third party has acquired the conversion table, it is extremely difficult to decrypt a message without the key. The point here is that since there is no restriction on the number of characters (frequency) that can be used as a key, an infinite number of keys can be conceived.

It took more than 100 years for the Vigenère cipher to develop from the conception to invention, but because simple substitution ciphers were still being used at the time and encryption and decryption with the Vigenère cipher were more difficult than with simple substitution ciphers, it took even longer for the Vigenère cipher to be adopted for practical use.

Uesugi Cipher

During the 16th century a cipher that involved the use of a Polybius square was created in Japan. The method of preparing encrypted messages is described in the book on the art of warfare written by Sadayuki Usami, a strategist of Kenshin Uesugi, who was a warlord during the Sengoku (civil war) period in Japanese history. This Uesugi cipher involved the use of a table comprised of 48 Japanese syllabary phonetic characters inscribed on a grid of seven rows and seven columns, with each character represented by the numbers across the top of each row and column. (Figure 4)

七	六	五	四	三	二	一	
ゑ	あ	や	ら	よ	ち	い	一
ひ	さ	ま	む	た	り	ろ	二
も	き	け	う	れ	ぬ	は	三
せ	ゆ	ふ	ゐ	そ	る	に	四
す	め	こ	の	つ	を	ほ	五
ん	み	え	お	ね	わ	へ	六
	し	て	く	な	か	と	七

Figure 4

4. Modern Ciphers: Ciphers during World War I and the Emergence of Encryption Machines

With the advancement of communication technology, encryption and decryption came to be actively performed during World War I.

German Communication Cables Disconnected by the United Kingdom

When the United Kingdom (U.K.) declared war on Germany at the start of World War I (WW I), the U.K. disconnected the German undersea communication cables, thereby making it necessary for the German forces to use international communication cables via the U.K. or wireless communications, and the German forces then started to encrypt their communications in an attempt to prevent hostile countries from reading them. The U.K., however, routed all intercepted communications to an agency called the Admiralty Intelligence Division, nicknamed “Room 40”, that was set up to decrypt encrypted German communications. One of its achievements was the decrypting of the Zimmermann Telegram.

Zimmermann Telegram

At the start of the WW I the participation of the United States in the European front impacted the outcome of the war. The Foreign Minister of Germany at the time, Zimmermann, conceived a scheme in which Mexico and Japan would launch attacks on the United States to dissuade the United States from participating in the war in Europe. Zimmermann directed the German Ambassador in Mexico to implement the attack, but the message was decrypted by Room 40. However, the U.K. decided not to divulge the contents of the message, in part because it wanted to prevent the Germans from designing an even stronger cipher upon discovering that the U.K. had succeeded in decrypting their messages. In the end, the U.K. provided the U.S. with a telegram in plain text that had been sent by the German Embassy in Mexico and been stolen by a spy who had gained access to the Mexican telegraph office. Upon receiving the telegram, the U.S. declared war on Germany and participated in the European Front.

The important point here is that a stronger ciphering method is developed each time a cipher is cracked. However, parties who succeed in cracking a cipher usually do not immediately reveal that they have, and instead continue to use the method for some time. As described below, it has led to repeated cycles of cipher creation and cracking in the modern era.

ADFGVX Cipher

The ADFGX Cipher, conceived by Colonel Fritz Nebel of the German Army, was first put to practical use in 1918. It involves the writing of five letters, ADFGX, in a column and a row, and replaces a character with two characters, and the encryption method is essentially the same as the Uesugi Cipher up to this point. The distinguishing feature of the ADFGVX cipher, however, is that the resulting series of letters is then ciphered again, this time by a transposition cipher method. The ADFGX Cipher was subsequently improved by using six characters, ADFGVX, instead of five (Figure 5), in order to make it easier to identify this cipher when messages were transmitted via Morse code.

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

Figure 5 ADFGVX Cipher

Ciphers that use such charts can be made practically impossible to decrypt by scrapping the key after using it just once, but since that means having to share an enormous number of keys with the frontline, delivering and receiving these keys has presented a major obstacle to using them in battle.

The Birth of Enigma

The difficulty of decrypting ciphers, which were prepared by hand before the 20th century, dramatically increased with the emergence of encryption machines at the start of the 20th century.

Enigma was the name of an encryption machine designed by the German inventor Arthur Scherbius in 1918, and it was marketed with portability and confidentiality as its sales features. Since the German forces had not yet learned that the cipher they were using in WW I had been decrypted when Enigma was first marketed, they were not aware of the need to improve their cipher, and because Enigma was very expensive, it was not adopted by the German forces.

When Germany later discovered that they had lost WW I as a result of their cipher having been cracked by the British, a sense of crisis developed in Germany, because they felt the fate of the nation rested on ciphers, and it was then that they decided to adopt Enigma.

The ciphering method used by Enigma is known as a polyalphabetic substitution cipher, and the “key” consists of a combination of gear wheels (rotors), known as “a scrambler”, on each of which 26 letters of the modern alphabet are inscribed, and a mechanism known as the plugboard for performing single character substitutions. Enigma is used by first setting the scrambler and then typing the plain (unencrypted) text on the keyboard of the Enigma machine. The ciphered letters, encrypted by the scrambler, are displayed on a lamp board. A single scale is rotated by the scrambler each time a character is typed, which means that a different key is used to cipher every single character.

Enigma decodes encrypted messages when the same key that was used to prepare the ciphered message is used to decrypt it, making it easy to decrypt as well as cipher.

The German forces continued to improve Enigma after adopting it by selecting three out of five rotors to comprise scramblers and by increasing the number of rotors accommodated from the original three to five.

Although the German forces had complete confidence in Engima, Poland, which was under threat of German invasion at the time, invented a decrypting system known in English as the “Bomb (cryptologic bomb)” that makes it possible to decrypt Enigma messages. For economic reasons, however, Poland was unable to keep pace with the increasing number of encryption patterns used by Germany as improvements were made to Enigma, making it impossible for Poland to continue its decrypting efforts. In 1939, Poland therefore provided the U.K., which had sufficient funds and personnel, with their research information and asked the U.K. to do the decrypting. Poland was invaded by Germany only two weeks later, and the World War II had begun.

The U.K. then began decrypting messages Germany created with the Enigma machine by using the information it had received from Poland. The discovery that the Germans were repeating the same three characters twice at the beginning of ciphered messages to specify the pattern (key) was the breakthrough in decrypting the Enigma messages.

The German information acquired by decrypting the messages encrypted by Enigma was referred to as “Ultra” by the U.K. and was an important source of information for the Allies until the end of the war. The decrypting of Enigma was kept a closely guarded secret, and the German forces continued to trust and use Enigma until the end of the war. (The decrypting of the Enigma cipher was made public in 1974, more than 20 years after it had been achieved.)

5. Modern Ciphers: Encryptions in the Computer and Internet Era

Since the end of the World War II the task of preparing and decrypting ciphers has shifted from machines to computers. The rapid popularization of computers in the private sector increased the need for encryption for private sector applications, such as commercial transactions between business enterprises, as well as for military applications.

DES Cipher

As illustrated by the example of the Enigma cipher described above, the decrypting of ciphers was treated with the strictest secrecy by nations. In 1973, however, the National Bureau of Standards (NBS, which later became the National Institute of Standards and Technology or NIST) of the U.S. Department of Commerce made a public call for a cipher method to be adopted as the standard by the U.S. Government.

The encryption algorithm, one of the two elements that comprise a cipher, i.e., the “encryption algorithm” and “key”, was disclosed. This was a historically significant switch for cipher. NBS approved the Data Encryption Standard (DES) cipher in 1976, and it became the global standard.

If an encryption method was set up for each individual use in the private sector, there would be a great burden on each business enterprise. In the 1970s, for example, when banks sent messages to their major clients, they handed the keys to their customers directly by their “key deliverer”. As the scale of banks’ business increased, and the number of keys that needed to be delivered increased with it, delivering keys became a management nightmare for banks. The disclosure of an encryption method therefore became the catalyst for resolving this problem.

Cipher has reached a historically important turning point involving the disclosure of the algorithm, use of the “key”, on the other hand, remained the same, because the “same key” was still used for both ciphering and decrypting (common key cryptography) the same as for a Caesar cipher or the DES cipher. The main problem with common key cryptography was how to deliver the key.

Public-Key Cryptosystem

A resolution to the problem of distributing keys, a problem since the time of the Caesar cipher, was finally achieved by the advent of the public-key cryptosystem. Whitfield Diffie, Martin Hellman, and Ralph Merkle anticipated the network computing era and undertook to resolve the problem of the public key. They presented the concept of a “public-key cryptosystem”, which, by using asymmetrical keys (public key and private key), makes it possible to encrypt communications without delivering a key in advance, at the National Computer Conference of 1976. The concept entailed making the encryption key available to anyone, whereas using a secret key that is known by only the recipient for decryption.

The key exchange concept devised by Diffie, Hellman, and Merkle has a modular arithmetic and one-way function, more specifically, the function $Y = A^X \pmod B$. This function means that A to the power of X divided by B leaves a remainder of Y. A common key is obtained by performing a calculation using the procedure described below, which provides an identical solution to both parties:

- **The values of A and B are shared by sender and recipient before transmission of a ciphered message. (As an example, let us assume that A = 7 and B = 11).**
- **X, which is known only to sender and recipient respectively, is then specified (In this example, let us assume that X = 3 and x = 6).**
- **The values of X and x and corresponding Y and y are calculated based on the shared values of A and B. (The resulting values for Y and y in this example are : Y = 2 and y = 4).**
- **Each party then supplies its own Y value to the other party.**

- **Each party then uses its own X value and the other party's Y value to once again perform a modular calculation to obtain the solution: (resulting in $Y^x \pmod{11}=2^6 \pmod{11}=9$, $y^X \pmod{11}=4^3 \pmod{11}=9$)**

The concept, which made it possible to carry on a conversation in public while assuring confidentiality, led to an innovative discovery that caused a significant rewriting of the fundamental principle that keys must be exchanged in secrecy.

However, it still has not been possible to find any one-way function that realizes asymmetrical ciphering, involving the use of different keys for ciphering and decrypting. The theory of this public-key encryption method has been applied in practice in the form of the "RSA Cipher".

RSA Cipher

Three researchers at the Massachusetts Institute of Technology, Ronald L. Rivest, Adi Shamir, and Leonard M. Adlemen, devised the mathematical method that was used to make the concept of a public key a reality, proposed by Diffie and Hellman. This public-key cipher is called the "RSA Cipher", with "RSA" being the initials of the last names of the three researchers who devised the mathematic method. The RSA cipher method utilizes prime factorization.

Prime factorization means factoring a number so that all its factors are prime numbers, (numbers that cannot be divided by any number other than one and itself), as illustrated in the examples given below:

95=5 × 19
851=23 × 37
176653=241 × 733
9831779=2011 × 4889

When this method is used in the public-key cryptosystem, the number on the left side of the equal sign is used as a portion of the public key and the private key. If it is a ridiculously large prime number, then it would be difficult to decrypt the prime number on the right side of the equal sign in a reasonable amount of time. Even though the details of the mathematical explanations are skipped here, needless to say, this characteristic of the prime factorization makes it difficult to decrypt the private key based on the public key.

Actually the cipher research institution in the U.K. invented a public-key cryptosystem before the RSA, but since it was considered a matter of utmost secrecy, because the invention of new ciphers was treated as a state secret, its existence was not made public until 1997.

The public-key cryptosystem is an extremely convenient system for exchanging keys to decrypt encryptions with a certain party or parties alone via the Internet. In other words, even though public keys are available to anyone on the Internet, to which any number of people have access, because it is difficult to decrypt the secret key within any reasonable time, for all practical purposes, the public-key cryptosystem can be viewed as a dramatic solution to the problem of distributing the key that had been a source of difficulty since ancient times.

Let us now briefly review SSL (Secure Socket Layer) as a method which made it possible to easily encrypt information made available over the Internet by anyone by using this common key cryptography together with the public-key cipher (RSA cipher). SSL is a protocol that was proposed by Netscape Communications and incorporated into Netscape Navigator, which made it possible for secure communications between a web server and a client.

The characteristics of SSL include the issuing of an electronic certificate that authenticates the identity of a server (web server or mail server), and is used for verification by the client before starting an SSL communication to ensure that it is explicitly indicated the communication is being initiated with the correct server. It also prevents data interceptions or leaks by encrypting subsequent communications.

The common key (in reality it is a random number that is the source of the common key) is safely distributed via the public-key cryptosystem to establish an encrypted data communication, and the issue of delivering the key has clearly been resolved using the public-key cryptosystem.

The public-key cipher method has a great advantage over the common key cryptosystem because of its ability to disclose the key publicly. The encryption process takes time, however, and uses a combined method of performing the message encryption using the common key supplied safely through the public-key cryptosystem.

Decrypting the DES Cipher

Returning to a previous topic, decrypting of the DES cipher is described in this section.

The DES cipher uses a 56-bit key, and since the number of combinations for 56-bit keys is 2 to the power of 56, which is roughly 70 quadrillion, it was considered nearly impossible to decrypt. Ultimately, however, it was decrypted in 1994. Modern encryptions have gradually become more susceptible to decrypting because of the recent significant improvements in the computational capacity of computers.

Responsive Action of Cipher Enhancements for SSL

There is a movement to change the specifications of the key length of public keys from 1024 bits to 2048 bits, as well as conform the public-key signature method to the SHA2 standard as a means of keeping pace with improvements in the computational capacity of computers. Schedules and policies regarding these issues have been determined by browser venders and authenticating authorities based on recommendations from the NIST, which formulates standard specifications for encryptions. Moreover, due to the compliance with the recommendations of the NIST by the Payment Card Industry Data Security Standard (PCIDSS), the SHA2 is attracting more attention from business enterprises that are considering supporting the PCIDSS.

For more information regarding the migration of 1024 to 2048-bit key length, visit our website at: http://www.thawte.com/resources/2048-bit-compliance/index.html

It is essential for those who use SSL encryption of communications to upgrade their client devices, such as personal computer browsers, cellular phones, smartphones and other devices, as well as web servers, early to those capable of dealing with new hash functions or responding to longer keys in order to sustain the encryption strength.

6. The Future of Encryption

As shown above the history of cryptography concerns the invention of encryption algorithms and the invention of decrypting methods. One of the cryptography methods that can be said to be currently attracting is “quantum cryptography”.

Quantum means the “minimum unit that can be measured”, and here it refers to a photon, i.e., a quantum of light. Photons vibrate as they move. Encrypted information can be received by measuring the angle of photon vibrations, and whenever a communication is intercepted by anyone other than the intended recipient, the angle changes, thereby ensuring that the interceptions will be detected.

The reason encryptions by quantum cryptography are considered impossible to decrypt, whereas encryptions in the past were considered “undecryptable within a reasonable amount of time”, is that the change in angle of the vibrations makes it possible to detect interceptions.

7. Conclusion: Enhancing the Effectiveness of Encryptions used for SSL

The encryption algorithms used for SSL are not incapable of being decrypted, they do not allow decrypting within a reasonable time and cost. Unless users apply the measures required by the characteristics and importance of the encrypted information, code breakers can decrypt the encryptions.

There have been periods throughout history when encryption methods were decrypted and no effective encryptions existed. In the modern era, the popularization of computers and the Internet have led to an encryption level unparalleled in the past and a situation in which the absence of effective encryption would seriously impact the use of the Internet.

Encryptions used for SSL can sustain their effectiveness provided that the encryption strength of the browser, server, and SSL certificate have all been enhanced to the same level, however, effectiveness cannot be sustained unless the encryption strength is enhanced, the same as with any other type of encryption.

It is important that both users and providers of information implement appropriate measures based on an adequate understanding of the characteristic of encryption, which is that “unless sufficient measures are implemented they will eventually be decrypted”.

References

Simon Singh, “The Code Book” (2001, Shinchosha)