Characteristics and Secure Use of Ciphers

Kazuyuki Nakagawa† *and Masayuki Kanda*

Abstract

Ciphers have become an essential means of defending against eavesdropping, falsification, and other threats to digital data including personal information. What is not well known, however, is that great care is required to select and operate ciphers in order to keep systems secure. This article describes the characteristics of ciphers and a method for achieving secure system operation using cryptographic technology.

1. Expanding use of ciphers

Without doubt, the Internet has become a major social infrastructure. In Japan, it has been pushed by a wide variety of governmental measures based on the e-Japan Strategy and the expansion of services in the private sector. At the same time, the flow of valuable information, such as personal information and business contracts, being transferred over the Internet is increasing. This, in turn, is increasing the risk of eavesdropping, spoofing by the sender/receiver of information, data falsification, and other Internet-related abuses. **Figure 1** outlines threats to digital data, categories and functions of ciphers for defending against those threats, and examples of applications that make use of ciphers. Ciphers are being used in a wide range of applications as described below.

(1) Improving the security of Internet communications

Various cryptographic schemes can be used to ensure that the other party in Internet communications is the proper one and to defend against eavesdropping. These include SSL (secure socket layer) communications between a Web browser and a Web server, Internet VPNs (virtual private networks) based on IPsec (IP security protocol), and security mechanisms in wireless local area networks.

(2) Maintaining the confidentiality of digital data

To comply with the act on the protection of personal information that went into effect in April 2005, companies in Japan are rapidly adopting data encryption schemes to prevent the leakage of information. The encryption of digital data stored on personal computers and the encryption of e-mail messages are typical examples of such efforts.

(3) Providing digital signatures for digital applications and contracts

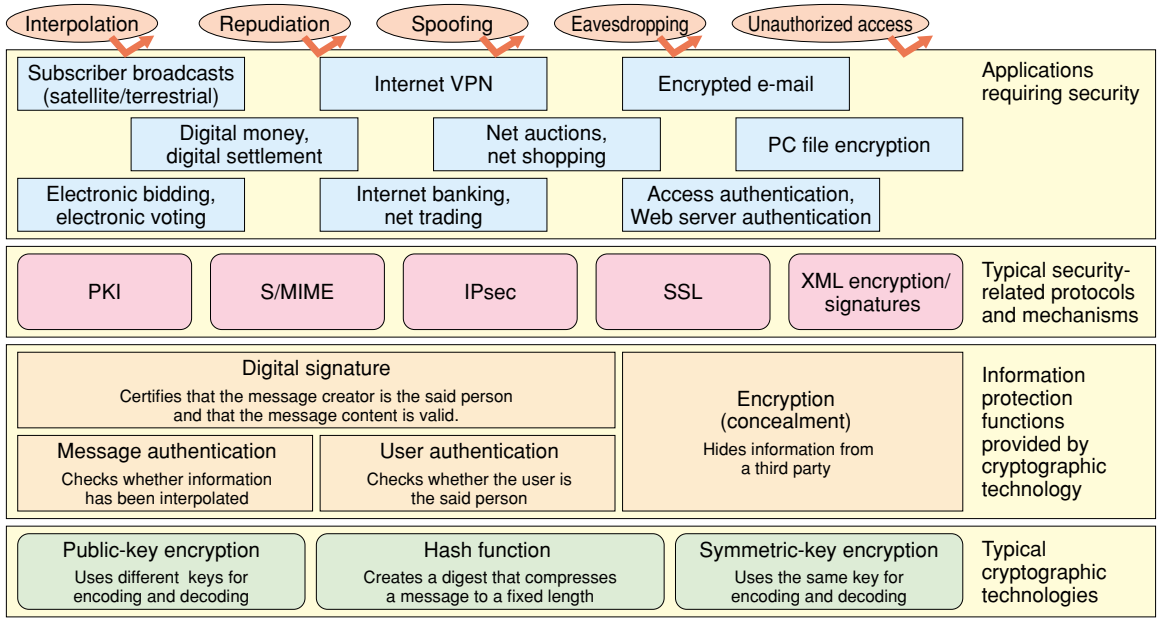
Digital applications, digital bids, and digital contracts are beginning to play an integral part in economic activities, so the information that they contain must be closely protected. Thus, in conjunction with authentication schemes to verify that an applicant or other party of a contract is actually the person claimed, there is a need for digital signatures to ensure that the contents of a digital application or contract on the Internet have not been falsified.

The functions of ciphers used in the above examples can be classified into three categories: encryption (concealment), user authentication, and message authentication. A digital signature provides both user-authentication and message-authentication functions.

2. Characteristics of ciphers

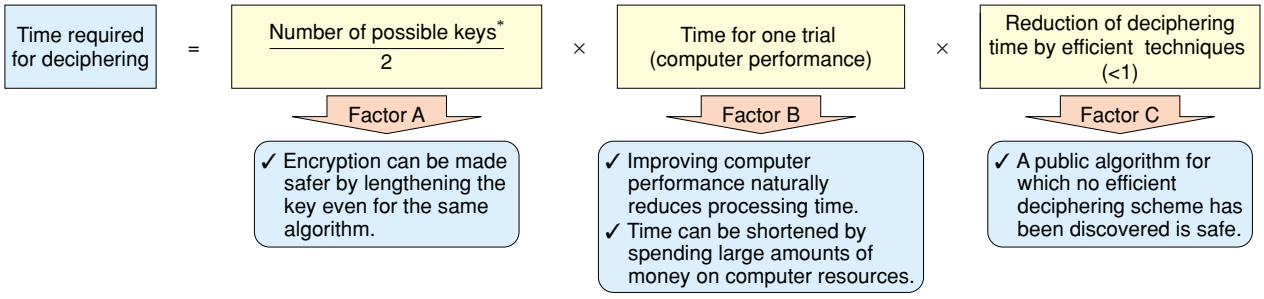
Though ciphers are essential for protecting valuable information from a variety of threats, it takes advanced mathematical knowledge to understand cryptography. In addition, it is not easy to discern

† NTT Department III
Chiyoda-ku, 100-8116 Japan
E-mail: security-info@ml.hco.ntt.co.jp



PKI: public key infrastructure, S/MIME: secure multipurpose internet mail extensions, XML: extensible markup language

Fig. 1. Threats on the Internet and protective cryptographic techniques.



Given that 10^{12} keys can be checked per second and that no efficient deciphering scheme has been discovered:

	(Factor A)	(Factor B)	(Factor C)	
♦ Deciphering time for a 56-bit key	= ($2^{55} \fallingdotseq 10^{17}$)	$\times 10^{-12}$	$\times 1$	$= 10^5$ s
	→ 28 hours			
♦ Deciphering time for a 128-bit key	= ($2^{127} \fallingdotseq 10^{38}$)	$\times 10^{-12}$	$\times 1$	$= 10^{26}$ s
	→ far longer than lifetime of the universe (70 billion years $\fallingdotseq 10^{11}$ s)			

Fig. 2. Breakdown of time required for deciphering.

whether the desired effect of protecting information has been achieved. Therefore, while many people are familiar with the term cipher, the reality is that they tend to use it without having a good understanding of its characteristics.

The underlying principle of modern ciphers can be described as follows: A person who knows the key for decoding ciphertext (encrypted data) can decode that data quickly, while a person having no knowledge of that key would require an impractical amount of computer power and time to decrypt the data. As shown in **Fig. 2**, the time required for cryptanalysis depends on three factors: key length of the cipher (Factor A), computer performance (Factor B), and efficient cryptanalysis techniques (Factor C).

(1) Key length of cipher

Keys have become increasingly longer over the years to make ciphers more secure. In symmetric-key encryptions, a key length of 128 bits is now mainstream. Figure 2 compares cipher breaking times for

key lengths of 56 bits (as used in DES (Data Encryption Standard)) and 128 bits (targeted for use in advanced encryption algorithms like Camellia and AES (Advanced Encryption Standard)). A 56-bit key would take just over a day to reveal, while a 128-bit key would take an impractical amount of time [1].

It must be pointed out here that the key length required for security depends on the type of cipher used. For symmetric-key encryption as in the above example, a key length of 128 bits is considered secure. On the other hand, for public-key encryption as in the RSA algorithm (named after Rivest, Shamir, and Adleman), a key should be from 1024 to 2048 bits to be secure because analytical techniques can be used against public-key encryptions and these are far more efficient than an "exhaustive attack" that tests all possible key values. This means that keys for public-key encryption must be much longer than those used for 128-bit symmetric-key encryption to achieve a comparable level of security.

(2) Computer performance

As described by Moore's law, computer performance can increase significantly from year to year, and as a result, ciphers that once required impractical amounts of time and money to break are becoming less secure as time passes. It is now becoming possible that such ciphers could broken in a realistic amount of time.

(3) Efficient cryptanalysis techniques

In contrast to exhaustive attacks, there has also been research to analyze the features of cipher algorithms with the aim of finding methods that can reduce the number of computations required for analysis. This is based on the idea that "in order to ensure the security of ciphers, a well-intentioned cryptographic researcher should investigate cryptanalysis techniques before a malicious person discovers them."

To give an example, the progress made by researchers in finding the factors of a composite number having a large number of digits is summarized in **Table 1**. Note here that the security of the RSA algorithm is based on the challenge posed by the huge number of calculations required to factor a many-digit composite number. The corollary of this, however, is that if one uses an RSA algorithm with a key length for which factorization is possible, then it is breakable. As a result, the RSA algorithm is currently used with using key lengths of 1024 bits or greater, and the need for key lengths of 2048 bits or greater is being debated.

Thus, a number of overlapping factors contribute to a decline in cipher security, making it unreasonable to expect a single cipher to be completely secure forever. It is therefore necessary to keep up with current trends in cryptanalysis techniques and use ciphers that are currently deemed secure. Without this kind of vigilance, the security of a system cannot be ensured no matter how much ciphers are used in that system.

Table 1. Progress in solving the prime factorization problem.

	Month/year	Number of bits*	Successful institution(s)
1	May 2005	663	University of Bonn
2	April 2005	582	NTT, Rikkyo University, Fujitsu Laboratories
3	Dec. 2003	576	University of Bonn, etc.
4	Dec. 2003	545	NTT, Rikkyo University, Fujitsu Laboratories
5	April 2003	530	University of Bonn

* Indicates the number of digits of the integer (in binary representation) for which prime factorization was successful.

3. What is cipher compromise?

A cipher becomes compromised when doubt is cast on its security. According to the "Survey on Cipher Compromise" issued by IPA/ISEC (Information Technology Promotion Agency Information Technology Security Center) in Japan [2], a cipher can be compromised when (1) the cipher algorithm is compromised as discussed above, (2) the cryptographic module is compromised by a defect in the cipher software or hardware, or (3) the system that uses the cipher is compromised because of poor cipher key management. Although the report is concerned with case (1), in which the cipher algorithm is compromised, care must also be taken over the cryptographic module and the system that uses the cipher.

The survey also divided compromised ciphers into five levels, as shown in **Table 2**. It can be seen that the fact that a cipher has been compromised does not necessarily mean that the system is immediately in danger. Because the danger of this type tends to increase gradually over time, system security can usually be ensured as long as appropriate information is collected and applicable measures are taken.

4. Method for using ciphers securely

As described above, having a clear understanding of cryptographic technology trends is essential in selecting and using a cipher algorithm. However, it is difficult to determine what cipher is secure without

Table 2. Levels of comprised ciphers.

Level 0	Safe	• No attack schemes have been reported.
Level 1	Check	• An attack scheme has been reported. • Cipher monitoring institutions have deemed it necessary to check the facts behind the above attack scheme and to maintain surveillance (status reports are issued by those institutions).
Level 2	Caution	• Existence of an attack scheme has been investigated and verified by a reliable source. • Based on the above investigation, cipher monitoring institutions have judged mainly from a theoretical viewpoint that the attack scheme will become credible in the near future (notices advising caution are issued by those institutions).
Level 3	Danger	• Existence of an attack scheme has been investigated and verified by several reliable sources. • Cipher monitoring institutions have judged that the above attack scheme will become a viable threat in the near future once it is applied to an actual operating system (declarations regarding this danger are issued by those institutions).
Level 4	Discontinue	• A ministry/agency-wide countermeasure-promotion institution has conducted an investigation on receiving the danger notice from cipher monitoring institutions and has decided that the cipher algorithm in question should be discontinued (discontinuation declarations are sent out by that institution). • Analysis of effects on e-government and plans for making a transition have been completed.

Extracted from "Survey on cipher compromise," March 2005, IPA/ISEC [2]

Table 3. Cryptographic-related institutions/projects around the world.

Institution name	Country/region	Summary	Related standards
NIST	United States	Establishes national standards for procurement by U.S. federal institutions and establishes standard cipher algorithms for the federal government.	Federal Information Processing Standards (FIPS)
CRYPTREC	Japan	Set up by MIC and METI as a joint project for evaluating encryption technology, these committees monitor the safety of cipher schemes recommended for use in Japan's e-government.	Recommended encryption schemes for e-government
IPA*1	Japan	An independent administrative institution providing software and strategic infrastructure functions to support the expansion of information-processing systems.	—
ECRYPT*2	Europe	A project established in 2004 to facilitate collaboration between researchers in Europe in relation to information security and especially cryptography and digital watermarks.	—
NESSIE	Europe	A project for evaluating cryptographic technology with the aim of establishing a strong portfolio of cipher schemes for diverse platforms.	Recommended encryption schemes for the European Union
KISA (Korea Information Security Agency)*3	Korea	An agency specializing in information security within the Ministry of Information and Communication that oversees Korean IT policies.	Encryption standards for the Korean government
ISO/IEC*4	—	An international standardization organization composed of representative standardization organizations from many countries. It creates international standards for all industrial fields.	ISO/IEC international standard cipher algorithms

*1 http://www.ipa.go.jp/
*2 http://www.ecrypt.eu.org/index.html
*3 http://www.kisa.or.kr/
*4 http://www.iso.org/iso/en/ISOOnline.frontpage

being an expert in the field. For this reason, the best method for the general user is to refer to the results of cipher monitoring and evaluation studies performed by cryptographic specialists. Major cryptographic-related institutions/projects around the world are listed in **Table 3**.

NIST (National Institute of Standards and Technology) in the United States [3] surveys international trends in cryptographic research and publishes Federal information processing standards (FIPS) on the cipher standards used by the United States government. These standards are reviewed every five years.

In Japan, as a result of evaluations performed by CRYPTREC (Cryptography Research and Evaluation Committees) [4] established by the Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, a list of recommended cipher algorithms for use in Japan's e-government was produced in February 2002 [5]. Similarly, NESSIE (the New European Schemes for Signatures, Integrity, and Encryption) project [6] announced recommended ciphers for the European Union also in February 2002.

Although the immediate objective of the above endeavors was to select ciphers for use by governments themselves or to provide a reliable list of secure cipher algorithms, the results can also be used by the private sector as guidelines for selecting ciphers to be used in commercial systems and products. But as pointed out above, both cryptographic technology and cryptanalysis techniques are always advancing, and it is important to keep up with cipher trends.

It is also important to consider the value of the information handled by a system and the number of years the system is expected to be used. Although the cost of carrying out an actual attack may be extremely high, for example, if a large number of computers are utilized, the extremely high value of the information handled by the system might make it worthwhile for malicious parties to mount such an attack. Furthermore, for a system having a service life of more than 10 years, the risk is high that the cipher used by the system will eventually be compromised even though it is currently judged to be secure. There are two effective measures that can be taken for such a system. The first is simply to use an up-to-date cipher algorithm judged to be secure. The second is to implement beforehand a mechanism that enables cipher algorithms to be easily exchanged in the event that the currently used one becomes compromised.

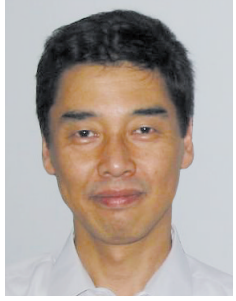
5. R&D toward secure use of ciphers

At NTT, many years of cryptography research have led to the development of a symmetric-key encryption algorithm called Camellia[*1], which is introduced in the fourth article in this special feature [7]. NTT is also researching methods of analyzing the factorization problem to help evaluate cipher security and is always collecting new information on worldwide cryptographic research and surveying the work of cryptographic monitoring organizations to provide up-to-date information to the NTT Group and outside enterprises. The results of these information-gathering activities will be used to develop a software library of cipher algorithms for future systems, to implement those algorithms in systems requiring advanced levels of security such as electronic authentication, and to expand applicable platforms such as smart cards and other devices.

*1 Camellia was developed jointly by NTT and Mitsubishi Electric Corporation.

References

[1] "Encryption and Authentication," November 2004, Nikkei Network (in Japanese).
[2] "Survey on Cipher Compromise," March 2005, IPA/ISEC (in Japanese).
[3] http://www.nist.gov/
[4] http://www.ipa.go.jp/security/enc/CRYPTREC/
[5] http://www.soumu.go.jp/s-news/2003/pdf/030303_3a.pdf (in Japanese).
[6] http://www.cosic.esat.kuleuven.ac.be/nessie/
[7] M. Kanda, "Promoting the Use of Camellia," NTT Technical Review, Vol. 4, No. 2, pp. 49-53, 2006 (this issue).



Kazuyuki Nakagawa
Senior Manager, Cyber Security Project, NTT Department III (R&D Strategy Department).
He received the B.E. and M.E. degrees in electro-communications engineering from the University of Electro-Communications, Tokyo in 1980 and 1982, respectively. In 1982, he joined the Yokosuka Electrical Communication Laboratories, Nippon Telegraph and Telephone Public Corporation (now NTT). He has been engaged in the development of integrated business communication systems and intelligent transport systems (ITS) and the planning of R&D strategy for the information sharing platform. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Masayuki Kanda
Senior Research Engineer, Information Security Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in electronic engineering from Tokyo Institute of Technology, Tokyo in 1991 and 1993, respectively. He received the Ph.D. degree in information engineering from Yokohama National University, Kanagawa in 2002. He joined NTT Laboratories in 1993. In 2002, he was temporarily transferred to the Telecommunication Advancement Organization of Japan. He has been engaged in the design and cryptanalysis of block ciphers and security protocols and in the promotion of Camellia. He is a member of IEICE and the Information Processing Society of Japan.