CRYPTREC Advisory Committee

Report 2002

March 2003

CRYPTREC Advisory Committee

CONTENTS

[Document]

Cipher Procurement Guidebook

[Reference]

Cipher usage policy for procurement of information systems at ministries and offices

1. Introduction

As exemplified by the rapid increase in Internet use, we are rapidly evolving into an IT (information technology) society. Based on the 'e-Japan Priority Policy Program,' the Japanese government aims, through administrative reform, to handle digital information in the same manner as paper information by 2003. This reform intends to make administrative procedures for such things as making applications, notifications, procurements, etc. more efficient thus streamlining administration and reducing burdens on the nation.

The increase of benefits brought about by IT development brings with it increasing risks and threats such as the emergence of new viruses and a higher risk of unauthorized access. In such an environment, the problem how to maintain the security and reliability of IT is a pressing issue we are now facing.

The Japanese government clearly recognizes that maintaining IT security is indispensable to the construction of a secure and reliable e-Government and that cryptographic techniques that form the foundation of information security technology are of great importance. This is also expressed in the 'e-Japan Priority Policy Program' determined (published?) by the IT Strategy Headquarters in March 2001. Further, in October 2001 it was decided in the IT security promotion meeting that the Ministry of Public Management, Home Affairs, Posts and Telecommunication and the Ministry of Economy, Trade and Industry (referred to as METI hereafter) will create a list of ciphers recommended for procurement in the 'e-Government' by the end of fiscal 2002.. This decision was based on the outcomes of study meetings convened by both ministries, and aims at an agreement on cipher usage policy among ministries and agencies.

Prior to this decision, the Information-technology Promotion Agency, Japan (IPA) established the CRYPTREC Evaluation Committee (referred to as 'Evaluation Committee' hereafter) to evaluate the security and implementability of cryptographic techniques available for e-Government. IPA also undertook administrative responsibilities for CRYPTREC in 2000, in response to a request from the METI (former Ministry of International Trade and Industry). In 2001, Telecommunications Advancement Organization of Japan (TAO) also participated in CRYPTREC. The CRYPTREC Advisory Committee (referred to as the Committee hereafter) was established in 2001 by the Director-General for Technology Policy Coordination, Minister's Secretariat, Ministry of Public Management, Home Affairs, Posts and Telecommunications (referred to as MPHPT hereafter) and by the Director-General of Commerce and Information Policy Bureau, METI. The purpose of this committee is, to have discussions on the usage of cryptographic techniques from a policy perspective.

The Committee is responsible for the investigation, research and evaluation of cryptographic techniques to be used in e-Government as well as those techniques egarding international standardization, and those used in accordance with the Law concerning Electronic Signatures and Certification. It is also responsible for the study of technical issues with regard to the usage of such cryptographic techniques. In 2002, the Committee completed evaluation of cryptographic techniques, formulated a draft of an e-Government recommended ciphers list, created a cipher procurement guidebook, and studied CRYPTREC activities for 2003 and the following years.

This report describes the results of the Committee's study conducted in 2002, and is to be reported to MPHPT and METI. It is intended that this report will be read by government employees who are involved in the construction of e-Government, as well as by general cipher users.

For more information on detailed technical matters in the 2002 CRYPTREC activities, please refer to the CRYPTREC Report 2002 provided by IPA and TAO based on the discussions at the Symmetric-key Cryptography Subcommittee and the Public-key Cryptography Subcommittee established under CRYPTREC and the Committee.

In 2002, the Committee attained its goal of creating a draft of an e-Government recommended ciphers list and a cipher procurement guidebook. However, in order to construct and operate an e-Government that people can use with ease, further investigation and evaluation of cryptographic techniques and establishment of security evaluation criteria for cryptographic modules is necessary.

Solid unity of persons involved in CRYPTREC and mutual cooperation are indispensable in proactively conducting the activities mentioned above. Therefore, further cooperation from persons concerned is kindly requested for the promotion of our activities as well as CRYPTREC activities.

In conclusion, I wish to express my deepest thanks to all the committee members, all the people participated as observers, all the Cipher Procurement Guidebook WG members who proactively created the guidebook, and all other people involved.

March 2003

Hideki Imai
Chairperson, CRYPTREC Advisory Committee

2. Background, Members and Details of Meetings of CRYPTREC Advisory Committee

2.1 Background of convening the committee

Maintaining security and reliability of advanced telecommunication networks is the foundation in creating the world's leading edge IT society, It is also a prerequisite for secure usage of communication networks by individuals. In the 'e-Japan Priority Policy Program' (determined on March 29, 2001 by the IT Strategy Headquarters) and 'e-Japan 2002 Program' (determined on June 18, 2002 by the Headquarters) based on the Basic Law on the Formation of an Advanced Information and Telecommunications Network Society, it is prescribed that the Government will take all necessary measures to eliminate interruptions of service provision due to threats in networks particularly in the e-Government, e-commerce and in major infrastructures.

Since cryptographic techniques form the foundation of IT security, their security must be evaluated objectively by technical specialists. To maintain security for the e-Government that is to be established by the end of fiscal 2003, the use of highly secure cryptographic techniques is essential.

To this end, MPHPT and METI intend to contribute to the construction of a secure and reliable e-Government that can be used by nations (?) with ease, by making a list of cryptographic techniques which are objectively judged to be superior in security and implementability. Government agencies will be encouraged to use such cryptographic techniques.

2.2 Organization of CRYPTREC

CRYPTREC, an abbreviation of Cryptography Research and Evaluation Committees, is a cryptographic technique evaluation project undertaken by the CRYPTREC Advisory Committee (chaired by Hideki Imai, professor of University of Tokyo) convened by MPHPT and METI, and by the CRYPTREC Evaluation Committee (also chaired by Hideki Imai) convened by TAO and IPA (see Fig. 1 for the CRYPTREC organization). Both Committees have conducted studies and evaluations as described below.

2.2.1 CRYPTREC Advisory Committee

The CRYPTREC Advisory Committee (referred to as 'the Committee' hereafter) offered suggestions for the use of ciphers to MPHPT and METI, and also made policy decisions regarding the use of ciphers in e-Government. The Committee is ready to pace working groups as needed to efficiently conduct in-depth study. In 2002, the Cipher Procurement Guidebook WG (leader: Ryoichi Sasaki, professor of Tokyo Denki University) was established, and the WG created a guide to smoothly procure ciphers recommended for the e-Government.

The Committee was convened as a study group by the Director-General for Technology Policy Coordination, Minister's Secretariat, MPHPT and by Director-General of Commerce and Information Policy Bureau, METI. Representatives from the Cabinet Secretariat, the National Police Agency, the Defense Agency, the Ministry of Justice, the Ministry of Foreign Affairs, the

Ministry of Finance and other agencies participated as observers.

2.2.2 CRYPTREC Evaluation Committee

The CRYPTREC Evaluation Committee (Evaluation Committee) conducted technical evaluations of cryptographic algorithms, reported the evaluation results and offered technical suggestions regarding ciphers to the CRYPTREC Advisory Committee. The Symmetric-key Cryptography Subcommittee (chaired by Toshinobu Kaneko, professor of Science University of Tokyo) and the Public-key Cryptography Subcommittee (chaired by Tsutomu Matsumoto, professor of Yokohama National University) were provided (?) under the Evaluation Committee.

his Committee was convened as a committee of TAO and IPA, and people from MPHPT, METI, the National Police Agency, the Defense Agency, the Ministry of Foreign Affairs, and other agencies participated as observers.

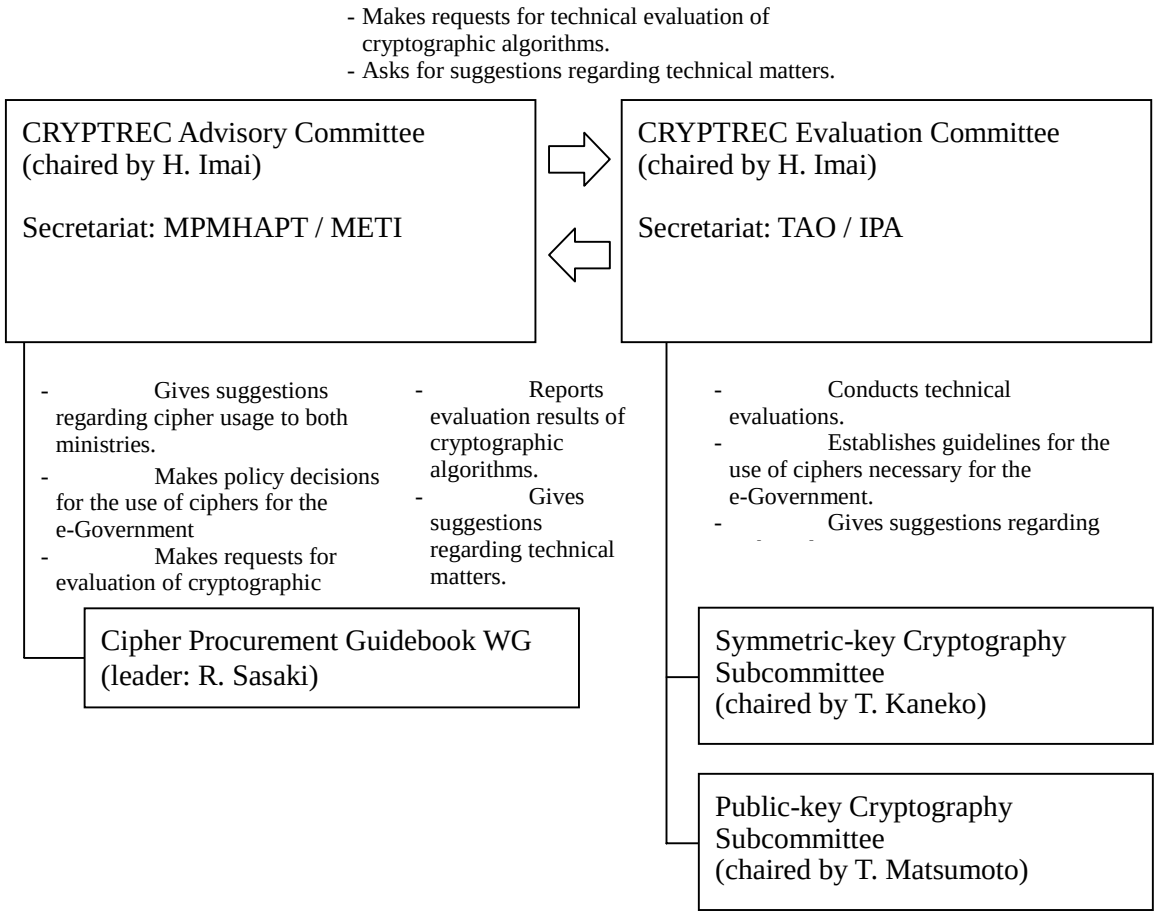


Figure 1 2002 CRYPTREC Organization

2.3 Committee members and WG members

2.3.1 CRYPTREC Advisory Committee members

[Members] *Titles, etc. as of the end of March 2003

Chairperson	Hideaki Imai	Professor, Institute of Industrial Science, University of Tokyo
Adviser	Shigeo Tsujii	Professor, Faculty of Science and Engineering, Chuo University
	Naoyuki Iwashita	Planner, Institute for Monetary and Economic Studies, Bank of Japan
	Hiroshi Okazaki	Senior Vice President, Communications and Information Network Association of Japan
	Eiji Okamoto	Professor, Information Sciences and Electronics, University of Tsukuba
	Tatsuaki Okamoto	Fellow, Nippon Telegraph and Telephone Corporation (Representative of Telecommunications Carriers Association)
	Masakazu Oda	Security Committee Member, Japan Information Technology Services Industry Association
	Ikuo Oyaizu	General Manager, Security Systems Group, NTT Electronics Corporation
	Yoshifumi Kato	Technical Committee Chairperson, Telecom Services Association
	Toshinobu Kaneko	Professor, Electrical Engineering, Science University of Tokyo
	Akio Kokubu	Director, New Media Development Association
	Koichi Sakurai	Professor, System Information Science Research Dept., Kyushu University
	Ryoichi Sasaki	Professor, Information Media Dept., Tokyo Denki University
	Kazuo Takaragi	IT Security Committee Member, Japan Electronics and Information Technology Industries Association
	Kenji Naemura	Professor, Faculty of Environmental Information, Keio University
	Mitsuru Matsui	Team Leader, Information Security Engineering Division, Mitsubishi Electric Corporation
	Tsutomu Matsumoto	Professor, Graduate School of Environment and Information Sciences, Yokohama National University

[Observers] *Titles, etc. as of the time of their participation

Junji Yoshihara	Cabinet Counselor, IT Security Office, Cabinet Secretariat
Shinki Tezuka	Manager, Info-Communications Bureau, National Police Agency
Noriaki Nakamura	Manager, Bureau of Defense Operations, Defense Agency (first meeting only)
Nobuyoshi Aoki	Manager, Director-General's Secretariat, Defense Agency (from second meeting)
Kuniomi Takamori	Manager, Administrative Management Bureau, Ministry of Public Management, Home Affairs, Posts and Telecommunications
Tomoyuki Sawatari	Planner, Local Administration Bureau, Ministry of Public Management, Home Affairs, Posts and Telecommunications
Haruo Nakagaki	Assistant Officer, Civil Affairs Bureau, Ministry of Justice
Masanori Ishikawa	Manager, Minister's Secretariat, Ministry of Foreign Affairs (first meeting only)
Kaoru Kusuda	Manager, Minister's Secretariat, Ministry of Foreign Affairs (from second meeting)
Minetaka Nakayama	Chief, Minister's Secretariat, Ministry of Finance (first meeting only)
Masao Uno	Planner, Ministry of Finance (from second meeting)
Tatsuo Kido	Chief, Industrial Technology Environment Bureau, Ministry of Economy, Trade and Industry
Hajime Fukuchi	General Manager, Information and Network Systems Div., Communications Research Laboratory (first meeting only)
Kazuo Hasuike	General Manager, Information and Network Systems Div., Communications Research Laboratory (from second meeting)
Kazuhito Omaki	General Manager, IT Research Institute, National Institute of Advanced Industrial Science and Technology
Kaoru Suzuki	General Manager, Telecommunications Advancement Organization of Japan (first meeting only)
Taku Kiyasu	General Manager, Telecommunications Advancement Organization of Japan (from second meeting)
Osamu Naito	General Manager, Security Center, Information-technology Promotion Agency, Japan
Akitoshi Yonekura	General Manager, Electronic Signature and Authentication Research Center, Japan Quality Assurance Organization
Hisayoshi Ogura	General Manager, Security & Audit Research Dept., The Center for Financial Industry Information Systems

2.3.2 Cipher Procurement Guidebook WG members

*Titles, etc. as of the end of March 2003

Leader	Ryoichi Sasaki	Professor, Information Media Dept., Tokyo Denki University
	Naoyuki Iwashita	Planner, Institute for Monetary and Economic Studies, Bank of Japan
	Naoki Ugamura	General Manager, IT Security Center, Japan Electronics and Information Technology Industries Association
	Eiji Okamoto	Professor, Information Sciences and Electronics, University of Tsukuba
	Shinichi Kawamura	Senior Research Scientist, Computer Network Laboratory, Toshiba Corporation
	Seiichi Susaki	Unit Researcher, System Development Laboratory, Hitachi Ltd.
	Makoto Tatebayashi	Team leader, Multimedia Develop Center, Matsushita Electric Industrial Co., Ltd.
	Itsukazu Nakamura	General Manager, Security Business Division, NTT Data Corp.
	Akitoshi Yonekura	General Manager, Electronic Signature and Authentication Research Center, Japan Quality Assurance Organization
	Hajime Watanabe	Researcher, IT Research Institute, National Institute of Advanced Industrial Science and Technology

2.4 Details of committee meetings

The Committee held six meetings in 2002. Date and major agendas of each meeting are as follows. For details of the Cipher Procurement Guidebook WG meetings, see Chapter 4.

[First meeting] May 16 (Thursday), 2002
(Main agendas)
- CRYPTREC Advisory Committee activity plan for 2002
- Number of e-Government recommended ciphers
- Requests to Evaluation Committee
- Establishment of Cipher Procurement Guidebook WG

[Second meeting] July 16 (Tuesday), 2002
(Main agendas)
- Guidebook draft for cipher procurement
- Number of e-Government recommended ciphers
- State of study for e-Government recommended ciphers list draft
- Current situation of cryptographic module evaluation

[Third meeting] September 30 (Monday), 2002
(Main agendas)
- e-Government recommended ciphers list draft
- Guidebook draft for cipher procurement

[Fourth meeting] November 27 (Wednesday), 2002
(Main agendas)
- e-Government recommended ciphers list draft
- Public comments for the list draft
- Guidebook draft for cipher procurement
- Current situation of cryptographic protocols (1)
- Future CRYPTREC activities

[Fifth meeting] February 12 (Wednesday), 2003
(Main agendas)
- Determination of e-Government recommended ciphers list
- Answers to public comments
- Guidebook draft for cipher procurement
- Current situation of cryptographic protocols (2)
- Future CRYPTREC activities

[Sixth meeting] March 24 (Monday), 2003
(Main agendas)
- Report for 2002
- Cipher procurement guidebook
- Future CRYPTREC activities

3. E-Government Recommended Ciphers List

3.1 Establishment of e-Government and evaluation of cryptographic techniques in 'e-Japan Priority Policy Program' and 'Security Action Plan'

The 'e-Japan Priority Policy Program determined （？） on March 29, 2001 by the IT Strategy Headquarters, defines the policy for promoting administrative informatization as the realization of an e-Government and the use of telecommunication technologies in public fields. Promotion of the standardization of cryptographic techniques is also stated as a concrete measure for maintaining the security and reliability of advanced telecommunication networks.

(Excerpt from 'e-Japan Priority Policy Program')

5. Promotion of administrative informatization and the use of telecommunication technologies in public fields

(2) Meaning of policy

--- (omitted) ---

Promote reformation of desk work, projects and organizations by administrative informatization, shift paper-based information management to electronic information management using networks while maintaining IT security especially in governmental organizations and agencies, in order to realize an advanced computerized administration, that is, an e-Government that involves the following:

(Main items) - Offering of administrative information as electronic data
- Computerization of application/notification procedures
- Computerization of revenues/expenditures
- Computerization of procurement procedures
- Shift from paper information to electronic information

6. Maintaining security and reliability of advanced telecommunication networks

(3) Concrete measures

(a) Formulation/improvement of systems/infrastructure regarding IT security

iii) Promotion of standardization of cryptographic techniques (MPMHAPT and METI)

Evaluate and standardize cryptographic techniques that will be available for the e-Government in 2002 through study meetings convened by specialists, while watching global standardization trends of cryptographic techniques at ISO, ITU, etc., in order to adopt cryptographic techniques provided with superior implementability and objectively evaluated security.

Following the determination of the e-Japan Priority Policy Program, 'Action plan for maintaining e-Government's IT security' was formulated under the initiatives of the Cabinet Secretariat, for the purpose of taking all possible measures to ensure IT security toward the creation of an e-Government in 2003. As a result, the action plan was determined (?)in the IT security promotion meeting on October 10, 2001. The plan states that a list of ciphers to be recommended for the procurement in e-Government must be made in 2002.

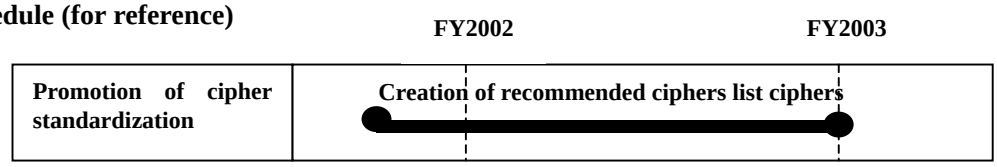
(Excerpt from 'Action Plan for maintaining e-Government's IT security')

2. Concrete measures

(2) Promotion of cipher standardization

- **It is essential for maintaining the security for the e-Government to use standards (ISO/IEC15408) for information processing equipment for maintaining a certain level of security in the procurement stage at the Government as much as possible, and also to use ciphers that have a certain level of security. Promotion of the use of such ciphers is necessary.**
- **To this end, MPMHAPT and METI <u>will create a list of ciphers to be recommended for the procurement in the e-Government in 2002 based on the outcomes of study meetings convened by both ministries, in order to agree on cipher usage policy among ministries and agencies involved.</u>**

Schedule (for reference)



In 'e-Japan 2002 Program' determined on June 18, 2002, 'establishment of an e-Government' and 'promotion of standardization of cryptographic techniques' are also stated as measures to be taken promptly and selectively by the Government for creating an advanced communication network society.

3.2 Evaluation of cryptographic techniques

3.2.1 Purpose of evaluation

In order to make computerized administrative procedures for applications, notifications and procurements available with ease, it is very important to evaluate cryptographic techniques[1] that are useful to the e-Government. Therefore, the CRYPTREC Evaluation Committee, which was established in 2000, has proceeded with a public invitation of cryptographic techniques, selection of cryptographic techniques, and has evaluated them.

This evaluation activity is the first step to the establishment of a cryptographic technique evaluation system, contributing to the international standardization of the cipher evaluation project NESSIE (New European Schemes for Signatures, Integrity, and Encryption) and ISO/IEC in Europe while referring to the AES (Advanced Encryption Standard) program that specifies the U.S. government standard ciphers.

3.2.2 Summary of evaluation

Cryptographic algorithms[2] were mainly evaluated during the evaluation of cryptographic techniques that will be available for e-Government. four categories of cryptographic techniques, public-key cryptosystems, symmetric-key ciphers, hash functions, and pseudo-random number generators were publicly invited and selected for evaluation, and then evaluated.

A two-step evaluation process consisting of a screening followed by a full evaluation, was conducted on the selected cryptographic techniques.

(1) Categories of cryptographic techniques
   i) Public-key cryptographic techniques
      Confidentiality, signature, authentication, and key agreement
   ii) Symmetric-key cryptographic techniques
      64-bit block cipher, 128-bit block cipher, and stream cipher
   iii) Hash function
   iv) Pseudo-random number generator

(2) Screening evaluation * not conducted in 2002
   Screening evaluation was conducted from the following viewpoints to judge whether full evaluation is necessary or not.
   i) Evaluate whether there are explicit problems with security or not.
   ii) Evaluate whether there are problems or not regarding implementation by a third party.

(3) Full evaluation

---

[1] : Cryptographic technique is a concept including cipher (cryptographic algorithm/cryptographic scheme), cryptographic protocol, cryptographic module, cipher key control, etc.

[2] : Cryptographic algorithm is simply referred to as cipher or cryptographic scheme.

Full evaluation was conducted for cryptographic techniques that were judged to be 'no problem' through the screening evaluation, from the following viewpoints in order to see if they have sufficient security or not for the e-Government.

i) Strength against known attacks

ii) Strength against attack particular to cryptographic techniques

iii) Criteria for setting parameters/keys

iv) Software implementation

v) Hardware implementation

3.2.3 Summary of evaluation criteria for each cryptographic technique

The evaluation criteria for each cryptographic technique are summarized as follows. For details of the evaluation criteria, refer to CRYPTREC Report 2002.

(1) Public-key cryptographic techniques

If a public-key cryptographic scheme[3] has a solid track record of operation and evaluation over a relatively long period of time and its specifications cannot be changed easily from the standpoint of interoperability, the following conditions must be satisfied: 1) the cryptographic techniques must have been evaluated and researched thoroughly by a number of researchers and 2) no security problems was reported in a realistic system.

For a relatively new public-key cryptographic techniques, we require them to have at least "provable security" because its specifications can be defined separately from existing cryptographic techniques. We carried out a comprehensive security evaluation in addition to checking the provable security, including issues such as the validity of number theoretic problems, method of selecting recommended parameters, and method of using auxiliary functions in a scheme.

(2) Symmetric-key cryptographic techniques

We require that symmetric-key cryptographic techniques should satisfy either of the following conditions.

(i) Even with the best attacking technique available to date, computational cost of 2^{128} or more (i.e. exhaustive search for a secret key) is required to break selected symmetric-key cryptographic techniques it. It is necessary for the techniques to be shown that they are secure against typical attacking techniques such as differential and linear cryptanalysis.

(ii) Widely used symmetric-key cryptographic techniques which have been evaluated in details and have no security problems in a realistic system, are selected. In this case, computational cost of 2^{100} or more is required to break them.

(3) Hash functions (See Chapter 4 for further information.)

We require that hash functions should satisfy either of the following conditions.

(i) Even with the best attacking technique available to date, computational cost to find the input value for a specific output value is not less than computational cost required for the exhaustive search. Also, even if the best attacking technique is used, computational cost to

find a pair of input values with the same output value is 2^{128} or more.

(ii) Widely used hash functions which have no security problems in a realistic systems and its hash length is160 bits or longer, are selected.

(4) Pseudo-random number generators (for further information, See Chapter 5)

We require that pseudo-random number generators should satisfy all the following conditions.

(i) The statistical properties are close to that of a true random number. An unknown output bit of the future or past is hard to predict from the known output bit history.

(ii) The seed size must be large enough to be secure against an exhaustive key search of the system that uses a pseudo-random number generator.

(iii) The statistical properties of pseudo-random number generators should pass a typical statistical test suite for randomness such as SP800-22.

3.2.4 Summary of cryptographic technique evaluation results

Summary of the 2002 cryptographic technique evaluation results is described below. For details of the evaluation results, refer to CRYPTREC Report 2002.

(1) Review of public-key cryptographic schemes[4]

i) DSA (signature)

DSA is an electronic signature scheme proposed and standardized by the U.S. NIST (National Institute of Standards and Technology), and is specified in the Guidelines on the Law concerning Electronic Signatures and Certification[5]. Its object identifier is 1 2 840 10040 4 3.

DSA's security depends on the difficulty of discrete logarithm problems on a finite field. Though its provable security is not indicated, it is empirically secure.

From the perspective of security, it is strongly recommended to select 1024-bit parameter 'p'. Users should follow the correction for pseudo-random number generators offered to FIPS PUB 186-2 (+ change notice 1) by NIST in October 2001.

ii) ECDSA (signature)

CRYPTREC evaluated ECDSA (ANSI X9.62) and ECDSA (SEC 1[6]). ECDSA (ANSI X9.62) is a signature scheme specified in the Guidelines on the Law concerning Electronic Signatures and Certification, and its object identifier is 1 2 840 10045 4 1.

ECDSA's security depends on the difficulty of discrete logarithm problems on an elliptic curve. Though its provable security is not indicated, it is empirically secure. No major security problem had been identified as of FY2002.

Elliptic curve parameters of ECDSA (SEC 1) are shown in SEC 1. No significant

---

4 : "Public-key cryptographic scheme has provable security" means that the non-reality of attacking the scheme can be demonstrated along with the framework of a standard security evaluation model in the cryptographic theory field. However, even if the non-reality is not demonstrated at present, the security of the scheme in not denied.

5 : This means the Guidelines for authorization for specific authentication based on the Law concerning Electronic Signatures and Certification (2001 Notification No. 2 of MPHPT, Ministry of Justice, and METI). This is abbreviated to "the Guidelines on the Law concerning Electronic Signatures and Certification."

6 : One of the technical documents provided by the Standards for Efficient Cryptography Group (SECG).

problem with these elliptic curves has been indicated. From the perspective of security, it is strongly recommended to select parameters equipped with prime factors whose group order is 160 bits or more. Research on the pseudo-random number generators submitted to FIPS PUB 186-2 (+ change notice 1) by NIST should be monitored.

iii) ESIGN (signature)

There are a number of specifications for ESIGN signatures. TSH-ESIGN was also evaluated to understand ESIGN (submitted cryptographic technique) well.

The primitive's security depends on the difficulty of the $n = p^2q$-type integer factoring problem. Though the ESIGN signature generating speed is faster than the RSA signature generating speed, modulus parameters for ESIGN must be larger than that of RSA to make the ESIGN primitive as secure as that of RSA primitive.

(a) ESIGN does not have provable security. Actually, forgery of a signature is possible with non-negligible probability when some particular parameters are used.

(b) TSH-ESIGN does not have provable security that is required for newly submitted techniques.

iv) RSA (signature, confidentiality)

There are a number of specifications for signature schemes using the RSA primitive: CRYPTREC evaluated RSASSA-PKCS1-v1_5 and RSA-PSS. Both RSASSA-PKCS1-v1_5 and RSA-PSS are signature schemes described in the Guidelines on the Law concerning Electronic Signatures and Certification, and their object identifiers are 1 2 840 113549 1 1 5 and 1 2 840 113549 1 1 10 respectively.

There are several specifications for confidentiality schemes using the RSA primitive: CRYPTREC evaluated RSAES-PKCS1-v1_5 and RSA-OAEP.

These four RSA schemes are empirically secure because they have been widely used for a long period and have been evaluated from multiple viewpoints.

(a) RSASSA-PKCS1-v1_5 is a signature scheme described in the Guidelines on the Law concerning Electronic Signatures and Certification. It does not have provable security.

(b) RSA-PSS has provable security that is essential to newly submitted techniques.

(c) Since RSAES-PKCS1-v1_5 has been used in SSL3.0/TLS1.0, its use is allowed for the time being. Though it is empirically secure, it does not have provable security and may be vulnerable to active attacks. Therefore, adequate protective measures must be taken in an actual operation environment.

(d) RSA-OAEP has provable security that is essential to newly submitted techniques.

The RSA primitive's security depends on the difficulty of the n = pq-type integer factoring problem. From the perspective of security, it is strongly recommended that modulus parameter n = pq of 1024 bits or more be used.

v) ECIES (confidentiality)

ECIES was submitted to CRYPTREC as ECAES in 2000, but was submitted with its cryptographic technique name changed to ECIES in 2001. There are several specifications for ECIES. CRYPTREC evaluated ECIES in accordance with the specifications described in SEC 1.

The ECIES's scheme specified in SEC 1 is vulnerable due to defects in the input to KDF function and in MAC handling, and therefore does not have provable security that is essential to newly submitted techniques.

vi) HIME(R) (confidentiality)

HIME(R) is a cryptographic technique submitted in 2001 as the improvement of HIME-1 and HIME-2 which were submitted in 2000.

The primitive's security depends on the difficulty of the $n = p^2q$-type integer factoring problem. To obtain security as high as the RSA primitive's in the HIME(R) primitive, modulus parameters slightly larger than that of RSA's modulus parameters must be used. It was judged that reliable HIME(R) specifications were not officially obtained as of September 2002 due to defects and vagueness in the specifications. Additionally, implementation by a third-party and interoperability of HIME(R) were not guaranteed. Even if HIME(R) specifications are reasonably defined by eliminating the vagueness in the specifications, some problems still remain in showing the provable security described in the self-evaluation report. Hence, the specifications were not considered to be perfect. Therefore, in September of 2002, we had not recognized provable security for HIME(R) that is required for newly submitted techniques.

vii) ECDH (key agreement)

ECDH was submitted to CRYPTREC as ECDHS in 2000, but was submitted with its cryptographic technique name changed to ECDH in 2001.

The ECDH's security depends on the difficulty of a discrete logarithm problem on an elliptic curve. Though its provable security against active attacks has not been indicated, it is empirically secure. When using this scheme, operational attention should be paid.

Elliptic curve parameters of ECDH (SEC 1) are specified in SEC 1. No significant problem with these elliptic curves has been indicated. From a security perspective, it is strongly recommended that parameters equipped with prime factors whose group order is 160 bits or more be selected.

viii) DH (key agreement)

There are a number of specifications for DH. CRYPTREC targeted ANSI X9.42-2001.
The DH's security depends on the difficulty of a discrete logarithm problem on a finite field. Though its provable security against active attacks has not been indicated, it is empirically secure. When using this scheme, operational attention should be paid.
From a security perspective, it is strongly recommended that 1024-bit (or more) parameter 'p' be selected.

ix) PSEC-KEM (key agreement)
PSEC-KEM was modified from PSEC submitted in 2000 to meet the KEM technique deliberated at ISO/IEC 18033-2, and was submitted in 2001.
The PSEC-KEM's security depends on the difficulty of the discrete logarithm problem on an elliptic curve. Since it has provable security with respect to the KEM technique, it can be said that using PSEC-KEM for the KEM (Key Encapsulation Mechanism)-DEM (Data Encapsulation Mechanism) construction is secure. However, research on the use of KEM in any other contexts has not been done sufficiently. Therefore, future research on this scheme should be carefully monitored.
CRYPTREC recommends that the elliptic curves specified in SEC 1 be used. No significant problem with these elliptic curves has been indicated. From the perspective of security, it is strongly recommended to select parameters equipped with prime factors whose group order is 160 bits or more.

(2) Review of symmetric-key cryptographic schemes

i) CIPHERUNICORN-E (64-bit block cipher)[7]
No security problem has been found so far. This cipher belongs to a slow processing speed group.

ii) Hierocrypt-L1 (64-bit block cipher)[7]
No security problem has been found so far. This cipher belongs to a fast processing speed group.

iii) MISTY1 (64-bit block cipher)[7]
No security problem has been found so far. This cipher belongs to a fast processing speed group.

iv) Triple DES (64-bit block cipher)[7]
We consider this cipher to be secure as long as it is guaranteed by FIPS, etc.

[7] If a longer block length can be used when constructing a new e-Government system, 128-bit block ciphers are preferable.

v) Advanced Encryption Standard (128-bit block cipher)
No security problem has been found so far. This cipher belongs to a fast processing speed group.

vi) Camellia (128-bit block cipher)
No security problem has been found so far. This cipher belongs to a fast processing speed group.

vii) CIPHERUNICORN-A (128-bit block cipher)
No security problem has been found so far. This cipher belongs to a slow processing speed group.

viii) Hierocrypt-3 (128-bit block cipher)
No security problem has been found so far. This cipher belongs to a fast processing speed group.

ix) RC6 Block Cipher (128-bit block cipher)
No security problem has been found so far. The fastest encryption is obtained with Pentium III, but the software processing speed greatly depends on the platform used.
The CRYPTREC Secretariat received a written notification dated October 16, 2002 from RSA Security Inc., saying that they will not conduct further activities for the promotion of RC6 due to the intellectual property problem.

x) SC2000 (128-bit block cipher)
No security problem has been found so far. This cipher belongs to a fast processing speed group.

xi) MUGI (stream cipher)
No security problem has been found so far. This cipher belongs to a fast software processing speed group.

xii) MULTI-S01 (stream cipher)
No security problem has been found so far. This cipher belongs to a fast software processing speed group.

xiii) RC4 (stream cipher)
No practical breaking technique has been reported so far with respect to RC4 with standard specifications (word length n=8, number of conditions: 256). However, a report was submitted saying that RC4 is not necessarily secure depending on the initial condition generated from the private key. Therefore, when using RC4, attention should be paid to the decision of the initial condition.
With regard to the use of RC4 in SSL3.0/TLS1.0, no security defect has been reported so far. But CRYPTREC believes that the 40-bit RC4 which generates initial condition using a 40-bit private key is not secure because the private key can be estimated, though 40-bit private key (40-bit RC4) and 128-bit private key (128-bit RC4) are available in the SSL3.0/TLS1.0 specifications.

(3) Hash function[8]

i) RIPEMD-160
No security problem has been found so far.

ii) SHA-1
No security problem has been found so far.

iii) SHA-256
No security problem has been found so far.

iv) SHA-384
No security problem has been found so far.

v) SHA-512
No security problem has been found so far.

(4) Pseudo-random number generator

i) PRNG in ANSI X9.42-2001 Annex C.1/C.2
No major problem has been identified so far in the practical use of Annex C.1 when parameters are set correctly. See 5.3.1 for correct parameter setting method.
We do not recommend Annex C.2 since it has been found to be vulnerable to the attack assuming a powerful adversary.

ii) PRNG in ANSI X9.62-1998 Annex A.4
We do not recommend this generator because of the large bias produced in the pseudo-random number output distribution (same as the one used for an attack on DSA, which uses the PRNG for DSA in FIPS PUB 186-2 Appendix 3) depending on the parameter.

iii) PRNG in ANSI X9.63-2001 Annex A.4
We do not recommend this generator because of the large bias produced in the pseudo-random number output distribution (same as the one used for an attack on DSA, which uses the PRNG for DSA in FIPS PUB 186-2 Appendix 3) depending on the parameter.

iv) PRNG for DSA in FIPS PUB 186-2 Appendix 3
An attack method, which requires the known signature of 222 and computation amount of 264 that have a biased distribution of {0, 1}, has been disclosed. This attack method can be prevented by restricting the number of times that a specific single key can be used to less than 2 million times when pseudo-random numbers are used by DSA. We do not recommend this generator as a generating method for pseudo-random numbers, however, because a large bias occurs in the random number output.

---

[8]: If a longer hash value can be used when constructing a new e-Government system, hash functions with a hash value of 256 bits or more are preferable. But this does not apply to cases where hash functions to be used are specified by the public-key cryptographic technique specifications or where necessity for interoperability arises.

v) PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1
No major problems has been identified during practical use so far, as long as the parameters are set correctly. Note, however, that the methods defined in the specification include methods that are not always secure. Therefore, when you use this generator, refer to CRYPTREC Report 2002 and select the appropriate usage.

vi) PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1
No major problems has been identified during practical use so far, as long as the parameters are set correctly. Note, however, that the methods defined in the specification include methods that are not always secure. Therefore, when you use this generator, refer to CRYPTREC Report 2002 and select the appropriate usage.

Since the evaluations conducted in 2002 were intended to evaluate security against attacks based on our current understanding of threats and vulnerabilities., the evaluation results do not guarantee such security in the future. Because of this, we are not responsible for damage or losses arising from using the evaluation results and other information described in this report.

3.3 E-Government recommended ciphers list

In the fourth meeting (November 27, 2002), a draft of e-Government recommended ciphers list was created using the cryptographic technique evaluation results reported by the Evaluation Committee. For the creation of the draft, based on the results of discussions at the Requirement Research WG, the following factors were considered: (1) cipher strength, (2) long-term (10 years) cipher security, and (3) history of cipher usage by the general public.

Public comments on the list draft were made at MPHPT and METI from November 28 to December 25, 2002. As the result of reviewing the collected opinions and comments at the fifth meeting (February 12, 2003), both ministries publicized the e-Government recommended ciphers list (shown later) on February 20, 2003.

The list includes 9 public-key cryptographic schemes (signature: 4, confidentiality: 2, key agreement: 3), 12 symmetric-key cryptographic schemes (64-bit block cipher: 4, 128-bit block cipher: 5, stream cipher: 3), 5 schemes for hash functions, and 3 schemes for pseudo-random number generators --29 schemes in total. Notes are added respectively to schemes to which attention should be paid when using them.

Following the determination of the e-Government recommended ciphers list which was based on the ‘Action plan for maintaining e-Government’s IT security’ (see 3.1), the‘Guidelines for using ciphers in the procurement of information systems at ministries and offices’ (see Reference) was accepted on February 28, 2003. , The Guidelines for Using Ciphers in the Procurment of Information Systems” is hoped to bring about an increase in approved cipher usage. According to the Guidelines, MPHPT and METI will conduct evaluations of the security and reliability of the ciphers listed if necessary, while watching the future advancement of telecommunication technologies. Therefore, both ministries will monitor the e-Government recommended ciphers in CRYPTREC. See Chapter 5 for details.

E-Government recommended ciphers list

February 20, 2003

Category of technique		Name
Public-key cryptographic techniques	Signature	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	Confidentiality	RSA-OAEP
		RSAES-PKCS1-v1_5 (Note 1)
	Key agreement	DH
		ECDH
		PSEC-KEM (Note 2)
Symmetric-key cryptographic techniques	64-bit block ciphers (Note 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES (Note 4)
	128-bit block ciphers	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	Stream ciphers	MUGI
		MULTI-S01
		128-bit RC4 (Note 5)
Others	Hash function	RIPEMD-160 (Note 6)
		SHA-1 (Note 6)
		SHA-256
		SHA-384
		SHA-512
	Pseudo-random number generator (Note 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

Prepared by MPHPT and METI

Notes:

(Note 1) Use of this is permitted for the time being because it was used in SSL3.0/TLS1.0.

(Note 2) On the assumption that this is used in the KEM (Key Encapsulation Mechanism)-DEM (Data Encapsulation Mechanism) construction

(Note 3) When constructing a new e-Government system, 128-bit block ciphers are preferable if possible.

(Note 4) Using the 3-key Triple DES is permitted for the time being under the following conditions:

1) It is specified as FIPS 46-3
2) It is positioned as the de facto standard.

(Note 5) It is assumed that the 128-bit RC4 will be used only in SSL3.0/TLS(1.0 or later). If any other cipher listed above is available, it should be used instead.

(Note 6) If any ciphers with a longer hash value are available when constructing a new e-Government system, it is preferable that a 256-bit (or more) hash function be selected. However, this does not apply in cases where the hash function to be used has already been designated according to the public-key cryptographic specifications.

(Note 7) Since pseudo-random number generators do not require interoperability due to their usage characteristics, no problems will be generated from the use of a cryptographically secure pseudo-random number generating algorithm. Therefore, these algorithms are examples.

3.4 Provision of information on e-Government recommended cipher specifications

The e-Government recommended ciphers list only describes the names of cryptographic schemes selected and evaluated by CRYPTREC. However, specifications of each scheme must be obtained through other means (?) (?). Furthermore, in order to procure e-Government recommended ciphersprocuers must be able to conveniently obtain the specifications of each scheme. The specifications of the ciphers are not maintained by CRYPTREC. They are maintained by the submitters of the cryptographic techniques, NIST or other entities.. Therefore, we took the following measures to provide procurers with information on the specifications of e-Government recommended ciphers.

i) Publicize the e-Government recommended cipher specifications on the TAO's website and the IPA's website.

ii) For those specifications which cannot be publicized on either website, the URL of a homepage where the specifications can be referenced will be indicated or directions on how to find the specifications on the TAO and IPA websites will be provided.

iii) In the case of ii), when specifications can no longer be viewed, there will be a message explaining the situation on the TAO and IPA websites.

4. Cipher Procurement Guidebook

4.1 Purpose of the Cipher Procurement Guidebook WG

Determination of the e-Government recommended ciphers list has made it possible for e-Government to adopt cryptographic algorithms with superior security and reliability. However, in order for those in charge of procurement at ministries and offices to properly select cryptographic algorithms that meet their applications, a guidebook that that explains the process of choosing a cipher in an easy-to-understand manner, is desired.

To this end, the 'Cipher Procurement Guidebook WG' (referred to as Guidebook WG hereafter) was set up under the CRYPTREC Advisory Committee in May 2002. The WG consists of cryptography researchers, security specialists, and specialists of system development (leader: Ryoichi Sasaki, professor of Tokyo Denki University). The WG created a guidebook for those in charge of procurement to procure approved ciphers for e-Government (referred to as Guidebook hereafter) in cooperation with the Evaluation Committee, Public-key Cryptography Subcommittee, and Symmetric-key Cryptography Subcommittee. (? End of sentence?)

4.2 How to create the Guidebook

4.2.1 Target audience

The guidebook is written with the needs of Cipher Procurement personnel in mind however, those less familiar with cryptography terms should also be able to understand it.

4.2.2 Contents

For those less familiar with cryptography, we have also included the following in out guidebook:

Because such readers as mentioned above are also targeted, we decided to include the following in the Guidebook.

(1) Explanation of procedure from choosing a cipher to selecting cryptographic algorithms
(2) Details of e-Government recommended ciphers
(3) Precautions on ciphers for preparing cipher procurement specifications (?)

4.2.3 Relation to procurement using ISO/IEC15408

For the construction of high-security information systems, an agreement to 'use as many products, etc. evaluated or certified following ISO/IEC15408 as possible' was made among ministries and agencies. However, ISO/IEC15408 does not mention requirements for selecting cryptographic techniques. For this reason, we intended to reference both this Guidebook and the 'procurement guidebook using ISO/IEC1540' (issued by the Office of IT Security Policy, METI) when determining security requirements and cryptographic requirements for procurement of e-Government.

4.2.4 Study method

We studied the above-mentioned contents using the following procedure and methods. With regard to the explanation of cryptographic algorithms and technical descriptions, we got great help from the Evaluation Committee and the Public-Key/Symmetric-Key Cryptography Subcommittees.

(1) Procurement/Information Systems Hearing
In order to understand the current situation of system procurement (especially cipher procurement) and requirements, we had hearings with persons in charge of procurement at ministries and offices and of information systems, and asked for their opinions on the first draft of the Guidebook.

(2) Survey of foreign e-Government system examples
We surveyed several examples of cipher procurement guidelines for foreign e-Government systems.

(3) Edition at sub-working group
The Guidebook draft was extensively edited by the sub-working group based on the hearing results, the foreign examples surveyed, etc. The sub-working group was convened seven times from June until August 2002.

4.2.5 Dates and agendas of Guidebook WG meetings

[First meeting] May 22 (Wednesday)
(Main agendas) - Meeting schedule
- Study items
- Confirmation of contents (draft) and tasks

[Second meeting] July 8 (Monday)
(Main agendas) - Framework of Guidebook (draft)
- Review of foreign e-Government examples

[Third meeting] July 19 (Friday)
(Main agenda) - Review of primary draft of Guidebook

[Fourth meeting] September 3 (Tuesday)
(Main agenda) - Review of final draft of Guidebook

[Fifth meeting] September 24 (Tuesday)
(Main agenda) - Review of final draft of Guidebook

[Sixth meeting] November 19 (Tuesday)
(Main agenda) - Determination of Guidebook (draft)

4.3 Overview of Guidebook

4.3.1 Overall system review and relation to cipher procurement

Since ciphers are used as a part of security measures when constructing an information system, risk analysis must be conducted prior to cipher procurement in order to know for what purposes ciphers should be used. (Fig. 1)

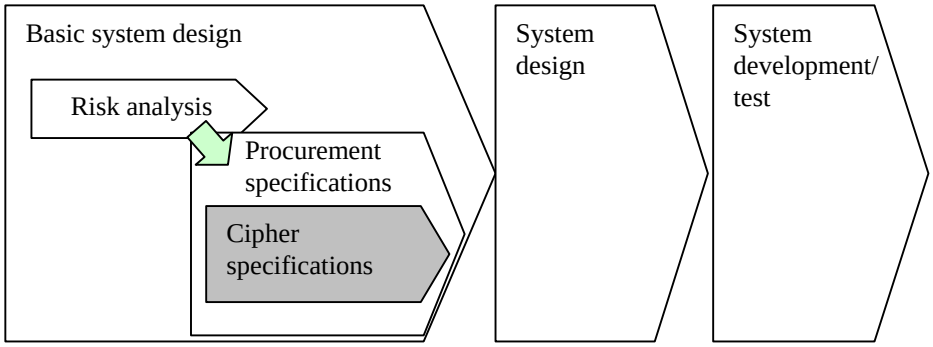
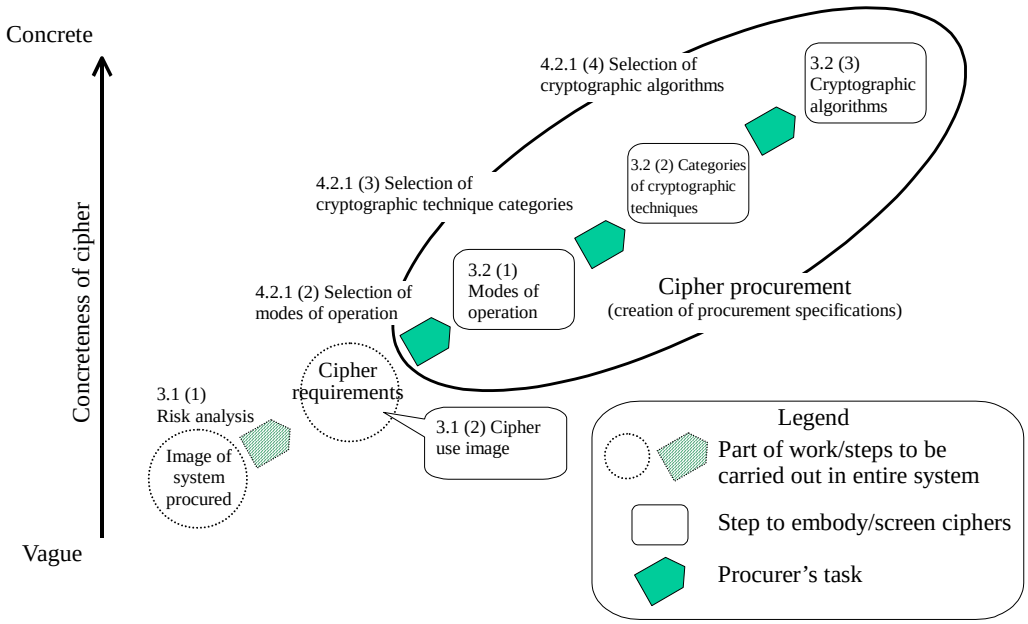


Fig. 1 System construction workflow and positioning of cipher procurement

Based on this risk analysis, cryptographic algorithms required for the system will be selected. Fig. 2 illustrates an example of the procedure. In this procedure, the Guidebook describes cipher procurement, modes of operation (a technical concept) necessary, categories of cryptographic techniques, and an overview of each cryptographic algorithm selected for the e-Government recommended ciphers.



*Numbers in the figure correspond to section numbers of the Guidebook

Fig. 2 Steps to the selection of cryptographic algorithms

4.3.2 Cipher use image （?） in an e-Government system

The Guidebook includes systems of ‘electronic application,’ ‘electronic procurement,’ ‘electronic payment,’ and ‘electronic information delivery’ as stated in the e-Japan 2002 Program. It also contains a cipher use image in the ‘Government’s authentication platform’ and its explanation.

4.3.3 Modes of operation and categories of cryptographic techniques

The Guidebook describes ‘modes of operation’ that categorize cipher use purposes for e-Government systems, and ‘categories of cryptographic techniques’ that arrange cryptographic algorithms in terms of functions and techniques.

4.3.4 Overview of e-Government recommended ciphers

The Guidebook summarizes 29 cryptographic algorithms selected for the e-Government recommended ciphers, as well as notes for using the algorithms.

4.3.5 Explanation of cipher procurement procedure

The Guidebook explains two models of cryptographic algorithm selection work, based on the Procurement/Information Systems.

(1) Cipher procurement workflow

Procurers must clarify cipher requirements for e-Government systems in the procurement workflow (Fig. 3 and Fig. 4), and then screen cryptographic algorithms from the e-Government recommended ciphers list. For screening cryptographic algorithms, the following two models are considered.

i) Procurer specified model

A method in which a system is described in detail when preparing procurement specifications and cryptographic algorithms are specified from the e-Government recommended ciphers list (?)

ii) Proposal examination model

A method in which only the summary of ciphers is described in the procurement specifications, and cryptographic algorithms are selected from the list by an entity concerned, and are examined using proposal documents(?)

The former model requires detailing of requirements for ciphers at the procurement specifications preparation stage, while the latter model requires the same work at the examination stage after receiving the proposal. Therefore, it is considered that the procurer’s tasks for cipher procurement will be equivalent throughout the system procurement.

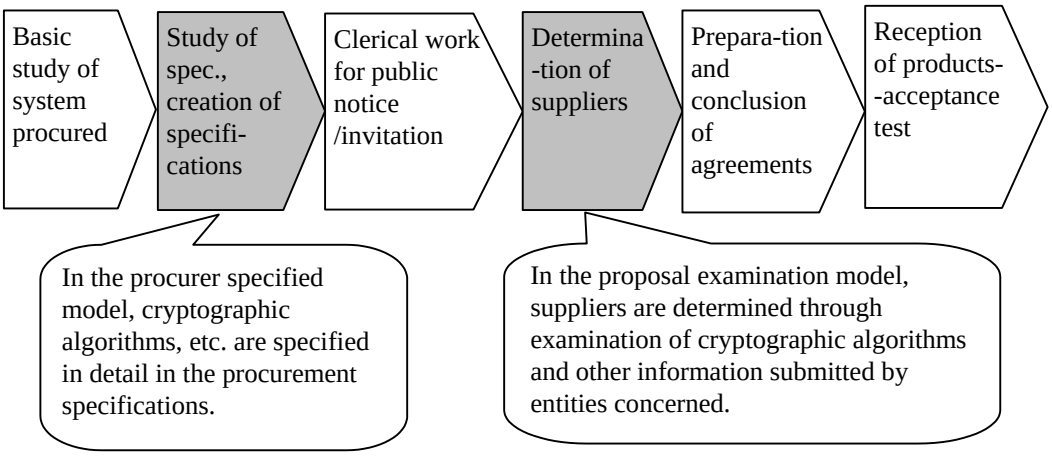


Fig. 3 System procurement workflow and positioning of two models

Procurement workflow	Outline of tasks
Basic study of system to be procured	Formulate basic matters for promoting procurement, such as system background, purposes, scope of targets, system construction conditions, cost estimate, and conduct risk analysis as a related task.
Study of spec./creation of procurement specifications	Study embodiment of system requirements and create system specifications (and solicit public comments if necessary).
Clerical work for public notice, public invitation, etc.	Carry out clerical work for public notice, public invitation, and acceptance of proposals.
Determination of suppliers	Select companies who offered a proposal that meets system requirements.
Preparation and conclusion of agreements	Prepare agreements including specific matters and enter into the agreements.
Reception of products -- acceptance test	Receive the system procured and verify compliance with specifications through acceptance tests.

Fig. 4 Outline of tasks in the system procurement workflow

(2) Creation of procurement specifications in the procurer specified model

Fig. 5 shows a cipher procurement workflow in the procurer specified model. The procurer analyzes the results (such as risk analysis results) of the system review, then selects modes of operation, categories of cryptographic techniques, cryptographic algorisms, and then completes the cipher procurement specifications.

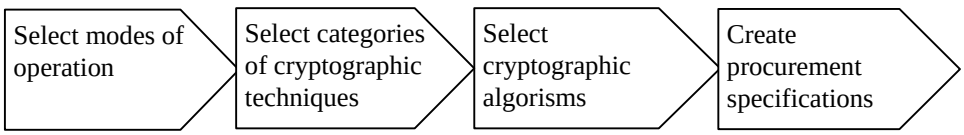


Fig. 5 Workflow in the procurer specified model

i) Selection of modes of operation

The Guidebook presumes that the selection of modes of operation will be carried out following the basic system (including risk analysis), and indicates general suggestions for selecting modes of operation against general threats.

ii) Selection of categories of cryptographic techniques

Following the determination of modes of operation, categories of cryptographic techniques will be selected, taking purposes/characteristics of the system into consideration. The Guidebook explains some examples for each mode of operation, in which symmetric-key cryptographic techniques and public-key cryptographic techniques are often used.

iii) Selection of cryptographic algorithms

Following the determination of cryptographic technique categories, the required number of cryptographic algorithms will be selected from the e-Government recommended ciphers list for each category. The Guidebook includes an 'Evaluation and Features List' for reference, which describes cryptographic algorithm security evaluation results, main requirements for parameters/auxiliary functions, and international standardization activities.

(a) Depending on how ciphers are implemented, threats due to various side-channel attacks cannot be eliminated, even if appropriate e-Government recommended ciphers are used. Therefore, adequate consideration, study, and proper measures against side-channel attacks are essential when implementing ciphers.

(b) Public-key cryptographic techniques will be selected according to modes of operation, while considering whether or not they have been adopted for protocol standard. It is necessary to study how to increase the key length (number of bits of a compound number that is the product of two prime numbers in the caser of RSA ciphers) to be used (1024 bits or more for RSA ciphers) within the range of permissible processing speed. Furthermore, care should be taken in the selection of parameters in order to maintain the number-theoretic difficulty of each algorithm.

(c) Symmetric-key cryptographic techniques will be selected based on processing speed, implementability in a restricted memory environment, and whether they have been adopted for protocol standards. When selecting block ciphers, 128-bit block ciphers should be used as much as possible. Several techniques called 'Modes of Operation' are specified regarding encryption processing using block ciphers, and purposes and functions vary according to each mode. Therefore, appropriate modes of operation will be selected according to the implementation environment or applications.

(d) It is preferable to select hash functions that output hash values with a bit length of 256 bits or more. However, if hash functions are specified in the specifications of public-key cryptographic techniques or symmetric-key cryptographic techniques selected already, select the most appropriate one.

(e) With regard to pseudo-random number generators, 'cryptographically secure pseudo-random number generating algorithms' other than the algorithms in the list are available. If the use of specific pseudo-random number generating algorithm is specified in the specifications of the algorithms listed, it will not effect the algorithm.

iv) Creation of procurement specifications

The following table shows an example of how to describe selected cryptographic algorithms in the procurement specifications (Fig. 6).

Information requiring cryptographic protection	Modes of operation	Cryptographic algorithm
- Application data - Data arrival checking notice sent/received upon checking application content - Data sent/received upon checking situation - Investigation end notice - Official document (permission, approval, etc.) request data - Official document (permission, approval, etc.)	Confidentiality	*Symmetric-key cryptographic technique (1)*
	Authentication of the other party	*Public-key cryptographic technique (1)* or *public-key cryptographic technique (3)*
	Signature	*Public-key cryptographic technique (1)* or *public-key cryptographic technique (3)*
Key information	Key agreement	*Public-key cryptographic technique (2)*
When nothing is specified for the above cryptographic algorithms, use the algorithm on the right	As a hash function	*Hash function (1)*
	As a pseudo-random number generator	*Pseudo-random number generator (1)*

Fig. 6 An example of specification of cryptographic algorithms for electronic application system[9]

(3) Creation of procurement specifications in the proposal examination model

In the proposal examination model, the procurer should include the following items in the procurement specifications.

i) Instructions regarding the use of e-Government recommended ciphers

Instructions will be issued to proposing entities to use as many e-Government recommended ciphers as possible for systems to be procured.

ii) Instructions regarding indication of reasons for selecting cryptographic algorithms

Since the procurer of the system must verify that cryptographic algorithms have been properly selected during the deliberation of proposal, he/she will or should provide easy to understand instructions that explain the process from system image to selection of cryptographic in the proposal.

[9] : Conduct proper procurements according to each specific situation without using the example itself in an actual procurement stage.

4.3.6 Precautions for creating procurement specifications

The following are precautions to be observed by procurers when creating procurement specifications.

(1) Regarding implementation of two or more cryptographic algorithms

When two or more cryptographic algorithms are implemented in a server, PC, etc. in an e-Government system, the following are valid as long as only security is considered.(?)

i) Advantages produced by implementation of plural algorithms

Though the possibility of occurrence of cipher breaking problems is, it is effective in terms of security to implement plural cryptographic algorithms for backup in the event that a ciphers is broken.

ii) Disadvantages caused by implementation of plural algorithms

When plural cryptographic algorithms are implemented for backup, a security hole may emerge in the switching portion, which may increase the vulnerability of the system and degrade the security level.

iii) Measures

Therefore, only when the risk of increased security vulnerabilitiesy is judged to be smaller than the risk of decryption of cryptographic algorithms, two or more cryptographic algorithms should be implemented.

In systems used by the general public via the Internet, if cryptographic algorithms used by users cannot be identified to one as a whole, any of plural cryptographic algorithms must be used by the server on the Government side in some cases. (?)In such a case, it is preferable for user's convenience to implement plural algorithms while paying particular attention to prevent security holes.

(2) Delivery of cipher programs and cipher export restrictions by Foreign Exchange and Foreign Trade Control Law

Delivery of programs including cryptographic functions to general users is controlled by Foreign Exchange and Foreign Trade Control Law based on the Wassenaar Arrangement.

The Guidebook describes steps to take in order to avoid violating this law..

4.3.7 Determination of suppliers, agreements and delivery of products

The Guidebook describes steps to take to ensure that proposals are submitted according to procurement specifications, determination of suppliers, agreements, and delivery of products.

4.3.8 References

(1) Cipher usage policy for procurement of information systems at ministries and offices
A document on the use of e-Government recommended ciphers, which was agreed among ministries and offices, is included in the Guidebook.

(2) E-Government recommended ciphers evaluation and features list
A list of algorithm security systems???(reasons for entry in the list), main requirements for parameters/auxiliary functions, state of adoption for international standards, etc., of e-Government recommended ciphers, is also included in the Guidebook.

5. Future CRYPTREC Activities

CRYPTREC attained its initial goalsof establishing an e-Government recommended ciphers list and creating a cipher procurement guidebook.. In order for individual nations to use e-Government systems with ease, continuous activities to maintain the security and reliability of e-Government systems are necessary. CRYPTREC recognizes that efforts to maintain such secure and reliable systems are of great importance. To this end, CRYPTREC set up an activity plan for near future.

5.1 Purpose and content of future CRYPTREC activities

5.1.1 Purpose

CRYPTREC will promote activities to maintain the security and reliability of e-Government systems through evaluations of cryptographic techniques and other related techniques.

5.1.2 Contents of activities

The following are CRYPTREC activities for 2003 and beyond. If necessary, CRYPTREC will discuss specific activity contents for them on all such occasions.(?)

(1) Monitoring e-Government recommended ciphers
CRYPTREC will monitor the performance of e-government recommended cipers. If necessary, CRYPTREC will advise users of patches or newly discovered vulnerabilities. The e-Government recommended ciphers list will be modified as necessary to reflect these changes.

(2) Investigation/examination for maintaining security and reliability of selected ciphers

i) Investigation/examination focusing on cryptographic algorithms
CRYPTREC will conduct investigations and examinations fon cryptographic algorithms and the difficulty of number-theoretic problems such as integer factoring problem.

ii) Investigation/examination focusing on cipher implementation techniques
CRYPTREC will also conduct investigations and examinations focusing on cipher implementation techniques such as side-channel attacks.

(3) Investigation/examination for revision of e-Government recommended ciphers list
CRYPTREC will conduct investigations/examinations necessary for future revisions of the e-Government recommended ciphers list (creation of a new list or abandonment of the current list), such as an investigation to see how ciphers are used in the e-Government. In that case, CRYPTREC will closely liaise with MPHPT, METI, and the manager meeting among administrative information system related organizations.

(4) Establishment of cryptographic module evaluation criteria
CRYPTREC will create evaluation criteria and test criteria for cryptographic modules.

5.2 The future of CRYPTREC

The organization of CRYPTREC will change in the following ways: the CRYPTREC Advisory Committee will continue in its current form. The 'Cryptographic Technique Monitoring Subcommittee' and 'Cryptographic Module Subcommittee' will now fall under the auspices of the Cryptography Advisory Committee. with the 'Cryptographic Technique Investigation WG' under the 'Cryptographic Technique Monitoring Subcommittee' (see Fig. 7).

The existing Evaluation Committee will be merged into the Cryptographic Technique Monitoring Subcommittee, and the Public-key and Symmetric-key Cryptography Subcommittees are to be merged into the Cryptographic Technique Investigation WG.

Positions, structure and functions of the Committee, Subcommittees, and the WG are as illustrated below.

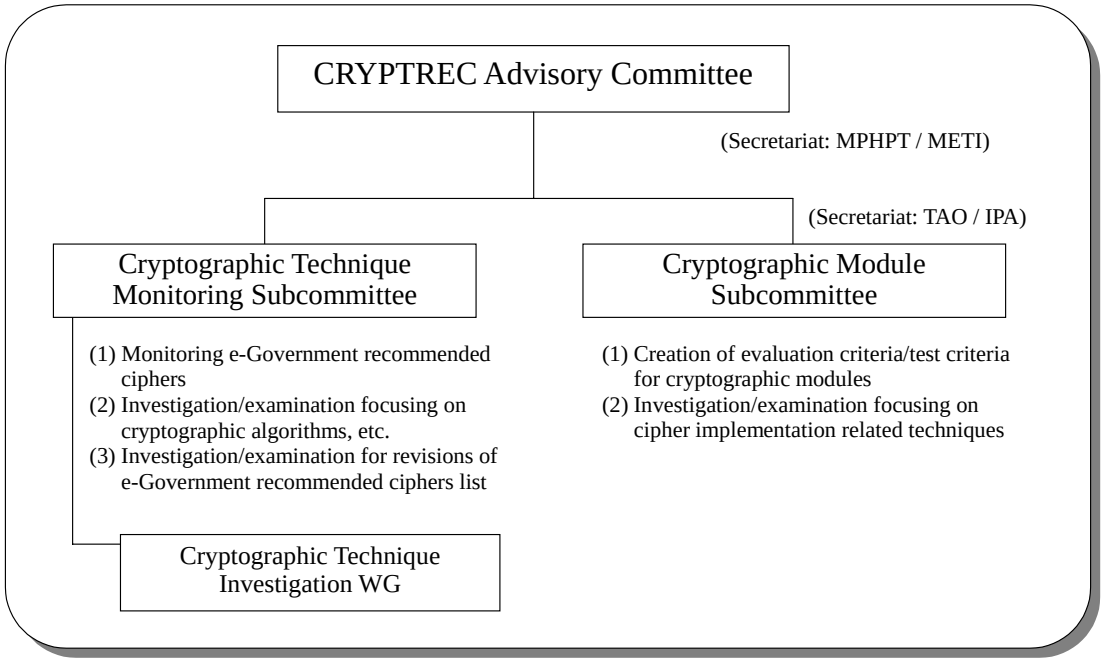


Fig. 7 Future CRYPTREC Organization

5.2.1 CRYPTREC Advisory Committee

The CRYPTREC Advisory Committee (the Committee) is responsible for the following: (1) monitoring of recommended cryptographic techniques, (2) related investigation and research, (3) comprehensive study on matters regarding evaluation/use of cryptographic techniques (such as vulnerability of cryptographic techniques and cryptographic algorithms), and (4) close liaison with security-related governmental organizations to maintain the security of e-Government.

5.2.2 Cryptographic Technique Monitoring Subcommittee

The Cryptographic Technique Monitoring Subcommittee (referred to as the Monitoring Subcommittee hereafter), consists of specialistsand is responsible for the following items: monitoring e-Government recommended ciphers to maintain their security and reliability; investigating/examining the cryptographic algorithms related to e-Government recommended ciphers; and the investigation/examination on revisions of the e-Government recommended ciphers list. The staff in charge of daily tasks of the Monitoring Subcommittee will be monitored by IPA and TAO/CRL (Communications Research Laboratory).TAO and CRL will merge in April 2004.

(1) Cryptographic Technique Investigation WG

i) Cryptographic Technique Investigation WG (refered to as Investigation WG hereafter) is placed under the Monitoring Subcommittee to provide support in preparing revision drafts of the e-Government recommended ciphers list.

ii) The Investigation WG is composed of Monitoring Subcommittee members, Evaluation Committee members, Symmetric-Key/Public-Key Cryptography Subcommittee members, and others. The WG members are divided into symmetric-key and public-key cryptography evaluation groups. The Monitoring Subcommittee convenes the symmetric-key cryptography evaluation group and/or the public-key cryptography evaluation group according to agendas to hold an Investigation WG. The WG offers specialized advice/suggestions on revision drafts of the e-Government recommended ciphers list, etc. to the Monitoring Subcommittee.

iii) The Investigation WG is convened upon request of the Monitoring Subcommittee to conduct specific investigation/examination focusing on cryptographic algorithms related to e-Government recommended ciphers (such as investigation of cipher usage situation in the e-Government). The WG will also provide the Monitoring Subcommittee with specialized advice and suggestions.

5.2.3 Cryptographic Module Subcommittee

The Cryptographic Module Subcommittee, under the direction of the CRYPTREC Advisory Committee, will establish cryptographic module evaluation criteria and test criteria by March 2005, while watching international standardization (ISO/IEC, etc.) trends and envisaging future use as a standard for governmental procurement. The Subcommittee will also investigate/examine cipher implementation related techniques, etc. for maintaining the security and reliability of the e-Government recommended ciphers.

5.3 Monitoring e-Government recommended ciphers

5.3.1 Basic idea on the monitoring of e-Government recommended ciphers

In order to maintain the security and reliability of the e-Government recommended ciphers, CRYPTREC will constantly monitor cryptographic techniques and, as required, monitor e-Government recommended ciphers to evaluate their security.

Monitoring will be carried out based on the following criteria:.

(1) E-Government recommended ciphers with security problems in the actual operation environment should be deleted from the list.

(2) Specifications of the e-Government recommended ciphers should not be changed.

(3) When the security of an e-Government recommended cipher can be maintained by simple modification of parameters, etc. which requires no specification change of the cipher, the cipher shall be left in the list with the modification information notified.

5.3.2 Details of monitoring

Monitoring of e-Government recommended ciphers is comprised of investigation/research, deletion from the list, and notification of modification information. Each of these is detailed below. (?)

(1) Investigation/research on cryptographic techniques and accumulation of data
Conduct investigation and research on cryptographic techniques, and accumulate various data on international standardization trends and others.

(2) Deletion of e-Government recommended ciphers

i) An e-Government recommended cipher will be deleted when it is judged that the cipher can be broken by attacks in the actual operation environment, and when it is judged impossible to avoid such attacks without changing the specifications of the cipher.

ii) An e-Government recommended cipher will be deleted when the possibility of breaking the cipher is deemed high in the actual operation environment and when it is judged that attacks can be avoided by simple modification of parameters, etc. without changing the specifications of the cipher, but when the modification information describing the method is not submitted by the manager of the cipher specifications.

(3) Notification of cipher modification information

i) The modification method will be released when the possibility of breaking of the cipher is deemed high in the actual operation environment and when it is judged that attacks can be avoided by simple modification of parameters, etc. without changing the specifications of the cipher.

ii) The Monitoring Subcommittee will require the manager of the cipher specifications to submit the modification information in the case of i), and shall evaluate the security of e-Government recommended ciphers taking the submitted modification information into account. If no modification information is submitted from the manager, the cipher shall be deleted from the list.

iii) The Monitoring Subcommittee will release the modification information when such modification information (simple modification only such as parameter change) has been submitted by the manager of the cipher specifications and when the Subcommittee judges that the security is ensured through evaluation taking the modification information into consideration, regardless that the Subcommittee does not judge that the possibility of breaking of e-Government recommended ciphers other than the submitted cryptographic techniques[10] is high in the actual operation environment.

(4) Addition of e-Government recommended ciphers

i) Addition of e-Government recommended ciphers should be treated as exceptional until the e-Government recommended ciphers list is revised (establishment of a new list or abandonment of the current list).

ii) When a cipher that is not included in the list gains high international evaluation and when the CRYPTREC Advisory Committee judges that the cipher must be evaluated newly and that the entry of the cipher into the list is appropriate, the cipher shall be added to the list.

iii) When examining the entry into the list, it shall be done from the perspective that the cipher is secure enough for 10 years or more.

[10] : Submitted cryptographic techniques mean the following among e-Government recommended ciphers.
(Public-key cryptographic techniques) ECDSA, RSA-PSS, RSA-OAEP, ECDH, PSEC-KEM
(Symmetric-key cryptographic techniques) CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000, MUGI, MULTI-S01

iv) When a request for adding a new application that is not included in the e-Government recommended ciphers list and/or for adding a new cipher suited for the application is made by the procurer of the e-Government, (??)and when the CRYPTREC Advisory Committee has judged such addition is appropriate and has selected a proper cipher based on the evaluation result of the cipher, such application and/or cipher shall be added in the list.

5.3.3 E-Government recommended ciphers monitoring procedure

The procedure of monitoring e-Government recommended ciphers consists of three steps all of which are conducted by the Monitoring Subcommittee: (1) information collection by the, (2) information analysis by the, and (3) deliberation and determination by the Monitoring Subcommittee in conjunction with the CRYPTREC Advisory Committee.

(1) Information collection by the Monitoring Subcommittee

In order to obtain information on security of the e-Government recommended ciphers, it is important to use the network with cryptography researchers formed through the 3-year CRYPTREC activities in addition to the information collection by the Monitoring Subcommittee itself.

i) Collect information on cryptographic techniques (scientific papers, announced documents) through participations in national and international academic meetings and in other opportunities.

ii) Strengthen the liaison network with the Investigation WG members to get necessary information constantly from them.

iii) Collect information on submitted cryptographic techniques from their suppliers as a rule.

iv) Collect necessary information from other general entities.

(2) Information analysis by the Monitoring Subcommittee

The Monitoring Subcommittee analyzes collected information and judges whether any situation requiring actions exists. If the Subcommittee judges such a situation has arisen, it convenes the symmetric-key cryptographic technique evaluation group and/or the public-key cryptographic technique evaluation group to hold an Investigation WG. However, when the Subcommittee judges that the situation is urgent, proper actions shall be taken in accordance with the situation.

(3) Deliberation and determination by the Monitoring Subcommittee and the CRYPTREC Advisory Committee

i) The Investigation WG offers advice/suggestions to the Monitoring Subcommittee from technical viewpoints. The WG also receives correction information from the suppliers of submitted cryptographic techniques, and conducts security evaluation of ciphers taking the correction information into account.

ii) The Monitoring Subcommittee prepares a preliminary draft describing whether any modification (deletion, etc.) of e-Government recommended ciphers is necessary or not, based on the advice/suggestions from the WG, and then reports the preliminary draft to the CRYPTREC Advisory Committee.

iii) The CRYPTREC Advisory Committee deliberates the preliminary draft from comprehensive perspectives and creates a draft regarding deletion of e-Government recommended ciphers, etc. When the draft causes any revision of the e-Government recommended ciphers list, MPHPT and METI add it to the Public Comment, and report the results to the CRYPTREC Advisory Committee. The Committee determines the draft taking the Public Comment results into consideration.

iv) When the e-Government recommended ciphers list has been revised according to the determination of the Committee, MPHPT and METI inform the manager meeting among administrative information system related organizations, etc. of the revision of the list.

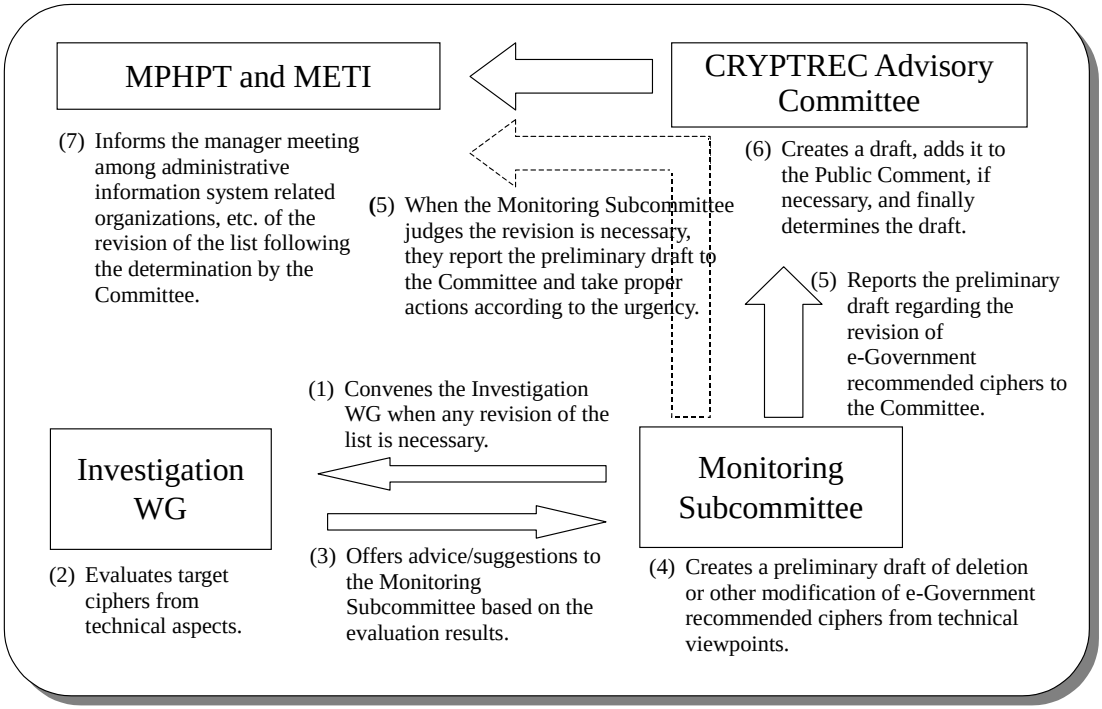


Fig. 8 Procedure for revising e-Government recommended ciphers list

5.4 Revision of e-Government recommended ciphers list

5.4.1 Basic understanding

The e-Government recommended ciphers were selected based on the concept that they can be used with ease for 10 years. However, cryptanalytic techniques and attacking techniques are advancing day by day, so the e-Government recommended ciphers are always exposed to dangers. On the contrary, new cryptographic techniques are also being developed and the emergence of new ciphers that are superior in security and implementability is expected. For this reason, it is preferable to periodically revise the e-Government recommended ciphers list by deleting vulnerable ciphers or adding new ciphers. If public invitation is carried out prior to revision, a period of five years or so is preferable from the announcement of public invitation (commencing date, invitation period, evaluation period, publication of new list announcement date) to the establishment of a new list.

5.4.2 Basic idea

Specific contents of the list revising work shall be discussed in a timely manner, while watching e-Government introduction state and e-Government recommended ciphers monitoring state. The following study items are prospected at present for revising the list.

(Study items prospected)

i) Necessity of public invitation

ii) Review of the list (categories of techniques, etc.)

iii) Number of ciphers in each category

iv) Evaluation criteria/evaluation methods

The revision work start time will be discussed and determined at the CRYPTREC Advisory Committee in 2003 or later. However, the revision work and the determination of a new list must be completed by 2013 at latest. Since a period of five years or so is preferable if public invitation is carried out, the public invitation should be announced by March 2008 at latest.

5.5 Study on cryptographic modules

Not only the security of cryptographic technique level but also the implementation security of cryptographic techniques must be ensured in order to keep the e-Government secure and reliable. To this end, it is urgently required to establish security evaluation criteria for cryptographic modules. With respect to such security evaluation criteria, the United States proposed the entry of FIPS140-2, a U.S. governmental procurement standard, in the ISO/IEC standards. Therefore, when establishing security evaluation criteria for cryptographic modules in Japan, discussions at ISO, IEC, etc. should be carefully monitored.

Considering such circumstances, Cryptographic Module Subcommittee is placed under the

CRYPTREC Advisory Committee. The Subcommittee will create evaluation criteria and test criteria for cryptographic modules by March 2005, while watching the trends of ISO and other international standards and envisaging adoption of them as governmental procurement standards.

The Subcommittee is also responsible for investigation/examination focusing on cipher implementation related techniques for maintaining the security and reliability of e-Government recommended ciphers, while liaising with the Monitoring Subcommittee.