CRYPTREC Project

Hideki Imai

Institute of Industrial Science, The University of Tokyo

http://imailab-www.iis.u-tokyo.ac.jp/

Foundations of the CRYPTREC

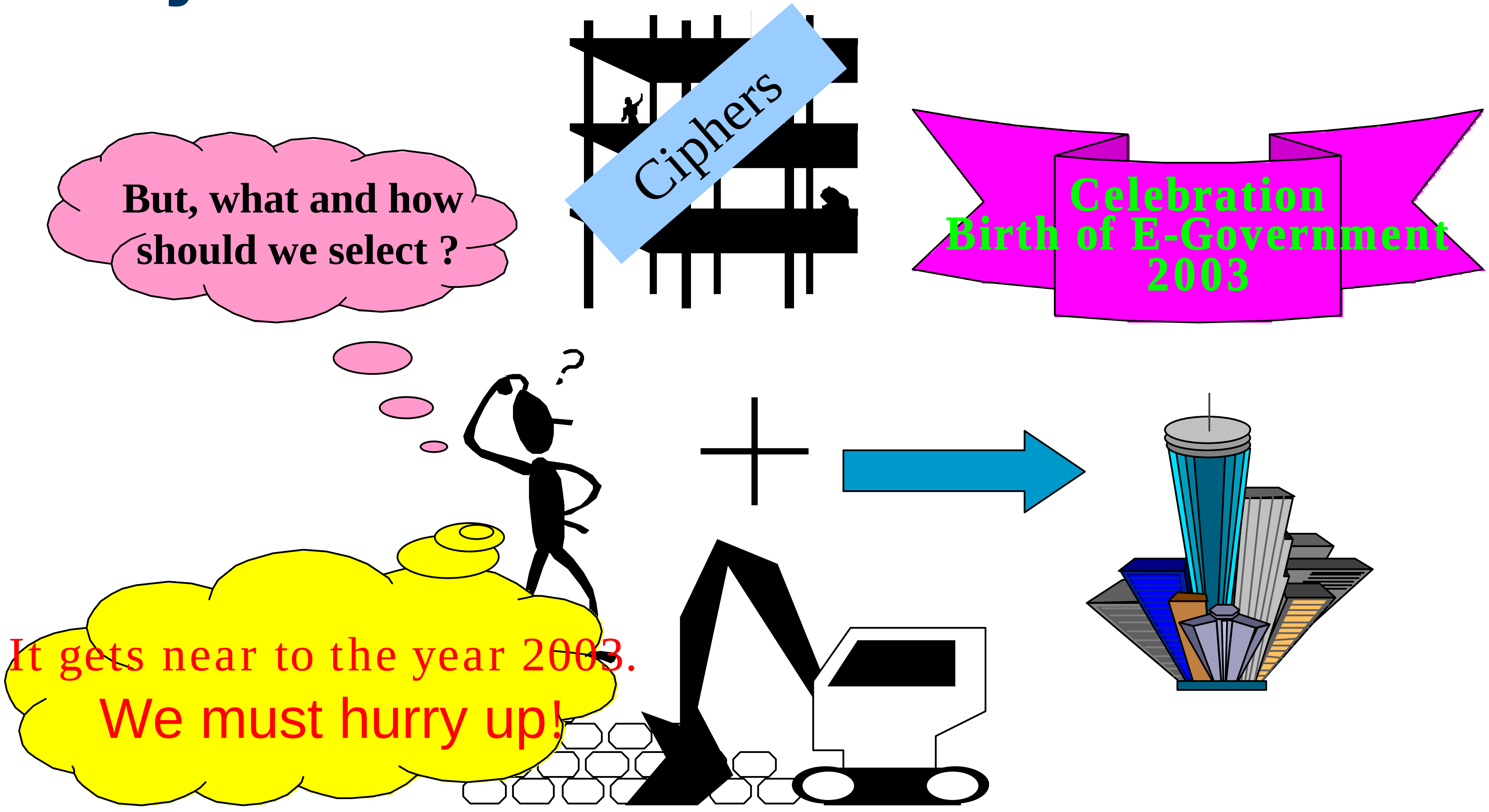
- Investigation and research of the Information-Technology Promotion Agency (IPA), JAPAN
  - CRYPTREC was established on the basis of the report of the consulting committee.
- Study Group for Promotion and Advancement of Encrypted Communications, MPT
- Launching examination on standardization of cryptographic algorithms by ISO
  - Coexistence with the registration scheme (based on ISO9979）?

This project is part of the Electronic Government Security Technology Development Project, which is sponsored by MITI and entrusted to the Information-technology Promotion Agency (IPA), Japan.

Motivation of the CRYPTEC Project

- Creation of the infrastructure for the electronic government by FY 2003
- Enhancing the security and reliability of the nationwide information network
- Recommendation of the OECD Council "Guidelines for Cryptography Policy"
  - PRINCIPLES 1. TRUST IN CRYPTOGRAPHIC METHODS
    - Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

Motivation of CRYPTEC Project



But, what and how should we select ?

Ciphers

Celebration
Birth of E-Government
2003

It gets near to the year 2003.

We must hurry up!

System Components

Activities of the CRYPTREC

- **CRYPTREC（Cryptography Research and Evaluation Committee）**
  - Secretariat ：Information-technology Promotion Agency, Japan Security Center http://www.ipa.go.jp/security/
- **Call for Cryptographic Technology**
  - The purpose of the project is to list valid cryptographic techniques together with
    - **Security profile, and**
    - **Implementation aspects.**
  - The list will be submitted to the government and open to the public.

Necessity of the CRYPTREC Project

- **Creation of the Infrastructure of the Electronic Government by FY 2003**
- **Assessment of the Security and the Implementation of Available Cryptographic Techniques to Achieve Information Security in the Electronic Government**
- **Trend of the Cryptographic Standardization**
  - ISO/IEC JTC1 SC27
    - From registration (IS-9979) to real standard
  - AES Project in USA
  - NESSIE (New European Schemes for Signature, Integrity, and Encryption)
    - The Information Societies Technology (IST) Programme of the European Commission

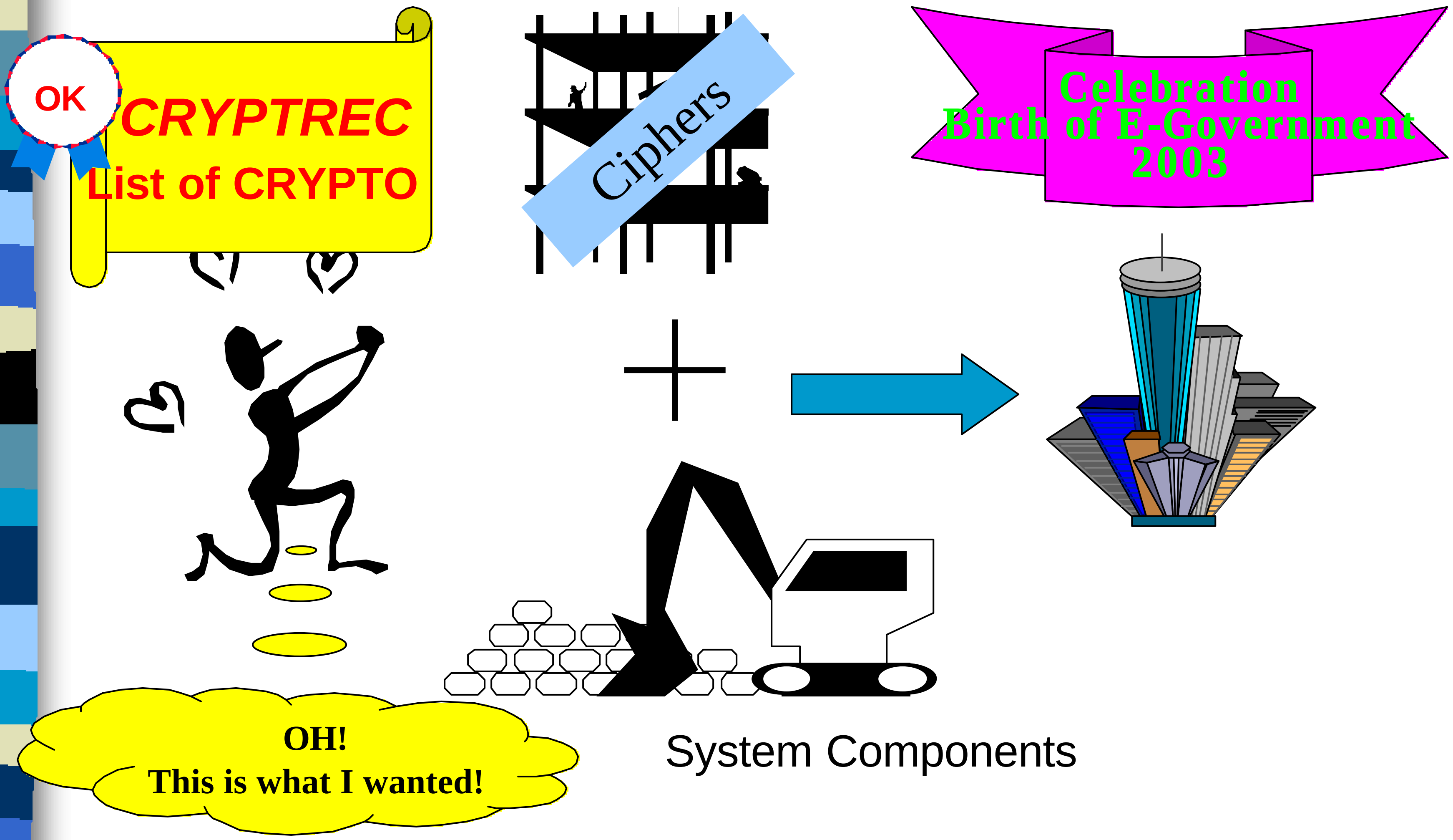
Goal of the CRYPTREC Project

- **Call for Cryptographic Techniques**
  - Available for the electronic government system
- **Proposed cryptographic techniques are evaluated from technical point of view by experts.**

→ **Technical Report Including a List of Analytical Results**

  - **Security Profile**
  - **Implementation Aspects**

Goal of the CRYPTREC Project



OK

CRYPTREC
List of CRYPTO

Ciphers

Celebration
Birth of E-Government
2003

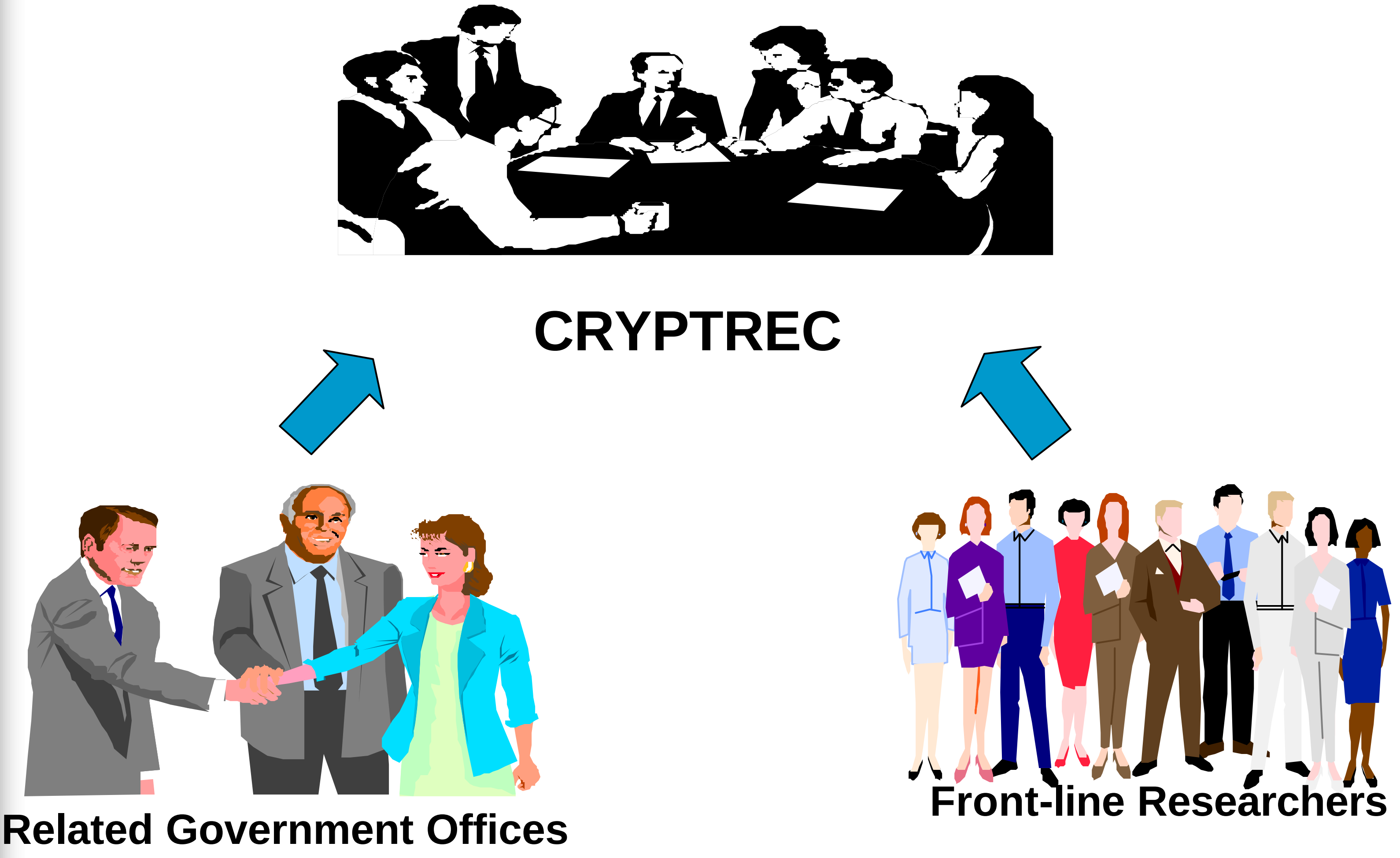
OH!
This is what I wanted!

System Components

Features of the CRYPTREC Project

- **Four related government offices participate in the CRYPTREC as observers:**
  - Management and Coordination Agency
  - Japan Defense Agency
  - Ministry of International Trade and Industry
  - Ministry of Posts and Telecommunications
- **Front-line researchers in the area of cryptology in Japan assembled.**
- **The balance of the security and the efficiency of implementation is among the top priority.**

Features of the CRYPTREC Project



CRYPTREC

Related Government Offices

Front-line Researchers

Organization of the CRYPTREC(1)

- **Members**

Hideki Imai	(University of Tokyo, Chair)
Naoyuki Iwashita	(Bank of Japan)
Eiji Okamoto	(Toho University)
Tatsuaki Okamoto	(NTT Laboratories)
Toshinobu Kaneko	(Science University of Tokyo)
Kouichi Sakurai	(Kyushu University)
Ryoichi Sasaki	(Hitachi, Ltd.)
Shigeo Tsujii	(Chuo University)
Kenji Naemura	(Keio University)
Mitsuru Matsui	(Mitsubishi Electric Corporation)
Tsutomu Matsumoto	(Yokohama National University)

Organization of the CRYPTREC(2)

- **Observers**

  Management and Coordination Agency

  Japan Defense Agency

  Ministry of International Trade and Industry

  Ministry of Posts and Telecommunications

- **Secretariat**

  Information-Technology Promotion Agency (IPA), JAPAN

Schedule

- **Schedule of the research and evaluation**

	2000							2001		
	6	7	8	9	10	11	12	1	2	3
Submission	←	→								
Screening evaluation			←	→						
Detailed evaluation					←	—	—	—	—	→
Announcement of results										☆

Procedure of Evaluating Cryptographic Techniques

- **Two-step Evaluation**
  - Screening evaluation
  - Detailed evaluation
- **Screening Evaluation**
  - Evaluation based on the submitted forms by entrusted experts
- **Detailed Evaluation**
  - Detailed evaluation by the entrusted experts including experimental examination
  - Voluntary evaluation by academic groups etc.
    - Technical information is open to public
    - Call for evaluation

Categories of Solicited Cryptographic Techniques

- **Asymmetric Cryptographic Schemes**
  - For confidentiality, authentication, signature, and key-sharing
  - Cryptographic schemes with primitives are invited

    Cryptographic primitive：an elementary cryptographic algorithm that provides security based on integer factoring problems, discrete logarithm, etc.

    Cryptographic scheme: an algorithm that provides one or more security functions by using cryptographic primitives and some auxiliary functions such as a hash functions.
- **Symmetric Ciphers**
  - Stream ciphers , 64-bit block ciphers,128-bit block ciphers
- **Hash Functions**
- **Pseudo-Random Number Generators**

Number of Applications for the CRYPTREC Call-Up

- **Asymmetric Cryptographic Schemes** : 24

– Confidentiality	7
– Authentication	1
– Signature	10
– Key-sharing	6

- **Symmetric Ciphers** :19

– Stream ciphers	6
– 64-bit block ciphers	4
– 128-bit block ciphers	9

- **Hash Functions** : 0
- **Pseudo-Random Number Generators** : 5

Screening Evaluation

- **Security Evaluation**
  - The schemes with evident critical defects are excluded from the detailed evaluation process.
- **Evaluation on the Implementation**
  - The following are excluded from the detailed evaluation process.
    - Proposal of a cryptographic technique not appropriate for the electronic government
    - Proposal not providing enough information for the third party to implement it

→ **Shortening the List of the Candidates for the Detailed Evaluation**

Result of the Screening Evaluation

- **Asymmetric Cryptographic Schemes** : 16

– Confidentiality	5
– Authentication	1
– Signature	6
– Key-sharing	4

- **Symmetric Ciphers** :12

– Stream ciphers	2
– 64-bit block ciphers	4
– 128-bit block ciphers	6

- **Hash Functions** : 0
- **Pseudo-Random Number Generators** : 1

Cryptographic Techniques for the Detailed Evaluation (1)

- **Asymmetric Cryptographic Schemes (Confidentiality)**
  - HIME-2(HITACHI)
  - EPOC(NTT)
  - PSEC(NTT)
  - ECAES in SEC1(FUJITSU & Certicom)
  - ACE Encryption(IBM)
- **Asymmetric Cryptographic Schemes (Authentication)**
  - ESIGN(NTT)

Cryptographic Techniques for the Detailed Evaluation (2)

- **Asymmetric Cryptographic Schemes (Signature)**
  - MY-ELLTY ECMR-OEF-h(MATSUSHITA)
  - MY-ELLTY ECMR-192-h(MATSUSHITA)
  - MY-ELLTY ECMR-160-h(MATSUSHITA)
  - ESIGN(NTT)
  - ECDSA in SEC1(FUJITSU & Certicom)
  - ACE Sign(IBM)
- **Asymmetric Cryptosystem (Key-sharing)**
  - HIME-1(HITACHI)
  - ECDHS in SEC1 (FUJITSU & Certicom)
  - ECMQVS in SEC1 (FUJITSU & Certicom)
  - HDEF-ECDH(JAIST & MATSUSHITA)

Cryptographic Techniques for the Detailed Evaluation (3)

- **Symmetric Ciphers (Stream Ciphers)**
  - MULTI-S01(HITACHI)
  - TOYOCRYPTO-HS1(TOYOCOM)
- **Symmetric Ciphers (64-bit Block Ciphers)**
  - CIPHERUNICORN-E(NEC)
  - MISTY1(MITSUBISHI)
  - FEAL-NX(NTT)
  - Hierocrypt-L1(TOSHIBA)

Cryptographic Techniques for the Detailed Evaluation(4)

- **Symmetric Ciphers (128-bit Block Ciphers)**
  - CIPHERUNICORN-A(NEC)
  - Camellia(NTT & MISTUBISHI)
  - RC6(RSA Data Security)
  - SC2000(FUJITSU)
  - MARS(IBM)
  - Hierocrypt-3(TOSHIBA)
- **Pseudo-Random Number Generators**
  - TOYOCRYPTO-HR1(TOYOCOM)

Reasons of the Exclusion (1)

- The proposed technique submitted to a category cannot be considered as a cryptographic technique in that category.
- The specification of the proposal is insufficient and cannot be interpreted as that of a cryptographic technique.
- The self-evaluation of the security was not enough to proceed to the detailed evaluation stage of the short period.
- The technology specification is not sufficient to implement the technique.

Reasons of the Exclusion (2)

- A critical defect in the security was pointed out.
- Short of the processing speed for the use of the electronic government.
- The proposal is evaluated in another category, because essentially the same cryptographic technique was submitted there.
- Documentation defect was found.
- Withdrawn.

Detailed Evaluation (Methods)

- **Evaluation by Foreign Researchers**
  - Reviewer: Eminent researchers in the area of cryptanalysis
  - Multiple cryptographic techniques are evaluated from the researcher's unique point of view.
- **Evaluation by Domestic Researchers**
  - Multiple cryptographic techniques are evaluated by each evaluation team**.**
  - Heuristic attacks to the candidate cryptographic techniques are surveyed and examined.
  - Performance when being implemented by hardware is evaluated.
- **Voluntary Evaluation by Academic Groups**

Other Important Cryptographic Techniques To Be Listed

- **CRYPTREC adds the following to the List:**
  - – Cryptographic techniques used in many systems,
  - – Cryptographic techniques indispensable for the application to the electronic government.
- **Cryptographic Techniques To Be Included**
  - – **Asymmetric Cryptographic Schemes**
    - RSA-OAEP, RSA-PSS, DSA, DH Key Exchange
  - – **Symmetric Ciphers**
    - AES(Rijndael)
    - Triple-DES
  - – **Hash Functions**
    - SHA-1, MD-5, RIPEMD-160
  - – **Pseudo-Random Number Generators (RNG)**
    - RNG based on SHA1

Detailed Evaluation (Criteria)

- **Security**
  - – Unified evaluation of the strength against the well-known attacks
  - – Evaluation of the strength against heuristic attacks
- **Implementation** （**Software & Hardware)**
  - – **SW**
    - Processing speed, resource amount, etc. are examined on the common platform.
  - – **HW**
    - Processing speed, amount of gates, etc. are examined on the common platform.

Evaluation Criteria (1)

- **Security of the Asymmetric Cryptographic Schemes**
  - Both schemes and primitives are evaluated.
  - **Evaluation Criteria of Schemes**
    - Possibility of passive attacks and active attacks
    - Effect of the attacks to the functions (confidentiality, authentication, signature, and key-sharing)
  - **Evaluation Criteria of Primitives**
    - Strength against the well-known attacks

Evaluation Criteria (2)

- **Security of Stream Ciphers**
  - Period, linear complexity, mutual information, etc.
  - Statistical characteristic **(**frequency, 0-1 balance, etc.**)**
  - Heuristic cryptanalysis
- **Security of Block Ciphers**
  - Well-known attacks (linear cryptanalysis, differential cryptanalysis, etc.)
  - Other attacks (higher order differential cryptanalysis, etc.)
  - Statistical characteristic (avalanche criterion, etc.)
- **Security of Pseudo-Random Number Generators**
  - Statistical property to the randomness tests such as the poker test, the long run test as described in FIPS140-1

Evaluation Criteria (3)

- **Implementation Evaluation**
  - Is it possible for the third party to implement the scheme on the basis of only the cryptographic technical specification document?
  - Is there any information that only the applicant knows ?
- **Design Criteria**
  - Are the design criteria of the key setting and the security parameters clear?

Cooperation with the Similar Projects Overseas

- **Sharing the Knowledge on Evaluation of Cryptographic Techniques with the Similar Projects**
  - Cryptographic Standard by the ISO/ I E C JTC1.
  - AES by U.S.A (NIST)
  - NESSIE by EU.
- **Cooperation and Harmonization from Various Aspects**

Summary and the Future Works (1)

- **Significance of the CRYPTREC Project**
  - It will provide reliable and proper information on cryptographic techniques required for the electronic government.
  - It will promote the development of cryptographic technology in Japan.
- **Status**
  - The screening process was finished.
  - The short list of the candidates for the detailed evaluation is available.
  - Detailed evaluation has started.

Summary and the Future Works (2)

- **Evaluation of the cryptographic technology must be continued.**
  - Permanent organization is necessary.
  - The target of this project is to evaluate the cryptographic technology that can be used in the electronic government in 2003.
  - The periods of the call-up and the evaluation are too short.
    - New cryptographic techniques and the improved ones should be evaluated.
- **The first step to the information security technology agency such as NIST and KISA.**