Trends in Cryptographic Techniques in Korea

Kyunghwan Park

Senior Member of Technical Staff
Cryptography Technology Team
KISA(Korea Information Security Agency)
khpark@kisa.or.kr

Cryptographic Techniques I

- Cryptographic techniques change rapidly due to
  - **The growth of the internet**
  - **The development of the computer technology**
- Cryptographic Techniques are needed to provide electronic security for
  - **e-government**
  - **e-business**
- The practical implementation of cryptographic techniques requires
  - **Interoperability => standardization**
  - **Efficiency => multi-platform**
  - **Security => public validation**

Cryptographic Techniques II

- Past
  - **It is developed secretly by the government for the military use**
  - **Government-driven standardization / De facto standardization**
- Present
  - **Develop: Public researchers**
  - **Validation : Public researchers and Government**
  - **De facto standardization / Government-driven standardization**

Korea

- Private Sector
  - **KISA, Cryptographic Technology Team**
    - **Government affiliated Agency under MIC(Ministry of Information and Communication)**
    - **R&D of related techniques and standard with Evaluation**
    - **Evaluation: Firewall, IDS**
      - Will evaluate all security products in the near future
    - **Root CA in PKI of Korea**
  - **ETRI(Electronics and Telecommunications Research Institute), Information Security Technology Division**
  - **KIISC(Korean Institute of Information Security & Cryptology), SIS(Standardization for Information Security) Research Group**
- Government Sector
  - **NSRI(National Security of Research Institute)**

Korea - Encryption standard

- SEED
  - A 128 bit block cipher with 128 bit key
  - 16 round Feistel structure
  - Faster then triple-DES
  - Developer : KISA
  - Developing Period : 1997.9-1998.12
  - Validation : KISA and Committee(consists of public researchers from KIISC)
  - Standard :
    - TTA (Telecommunications Technology Association) standard (1999.9) (=government standard)
    - Submit as ISO/IEC encryption standard (2000.9)
  - Among 38 opened industrial implementations in private sector : SEED 71%, DES 84%, RSA 63%

Korea – Digital signature standard

- **KCDSA** (Korean Certificate-based Digital Signature Algorithm) based on discrete logarithm problem
  - Developer : KISA and KIISC-SIS
  - Developing period :1994–1998
  - Standard : • **TTA standard(1998.10)**
    - **As a contribution to IEEE P1363a(1998.8)**
- **EC-KCDSA** (Elliptic Curve version of KCDSA)
  - Developer : KIISC-SIS
  - Developing Period : 1997–2000
  - Standard : • **TTA standard(2000.12 expected)**
    - **Contained in FCD 15946-2 with EC-DSA & EC-GDSA**

Korea – Hash function standard

- **HAS160** (Hash Algorithm Standard **with 160-bit output**)
  - Developer : KISA and KIISC-SIS
  - Developing period : 1995-1998
  - Standard
    - **TTA (Telecommunications Technology Association) standard (1998.10)**
  - Used as hash function in KCDSA

- **Sites for cryptographic standards in Korea**
  - http://dosan.skku.ac.kr/~sjkim/kg_std.html
  - http://oberon.postech.ac.kr/kiisc-sis/

World

AES - Round 1

Name	Nation	Submitter	Rounds/structure
CAST256	Canada	Entrust Tech., Inc.	48(12)/Modified Feistel
Crypton	**Korea**	**Future Systems, Inc.**	**12/SP**
DEAL	Canada	Richard Outerbridge	6,6,8/Feistel
DFC	France	CNRS	8/Feistel
E2	Japan	NTT	12/Feistel
FROG	Costarica	TecApro Internacional S.A.	8/Key Interp.
HPC	U.S.A.	Rich Schroeppel	8/Omni
LOKI97		Lawrie Brown, Josef Pieprzyk, Jennifer Seberry	16/Feistel
MAGENDA	Germany	Deutsche Telekom AG	6, 6, 8/Feistel
MARS	U.S.A.	IBM	32(16)/Modified Feistel
RC6	U.S.A.	RSA Lab.	20(10)/Modified Feistel
RIJNDAEL	**Belgium**	**Joan Daemen, Vincent Rijmen**	**10, 12, 14/SP**
SAFER+	U.S.A.	Cylink Corporation	8,12,16/SP
SERPENT	English, Israel, Norway	Ross Anderson, Eli Biham, Lars Knudsen	32/SP
TWOFISH	U.S.A.	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson	16/Feistel

World

- ISO/IEC
  - Korea submit following symmetric encryption algorithms as a candidates
    - SEED : by KISA
    - Xenon, Zodiac : by SoftForum Co.
  - EC-KCDSA is included in FCD 15946-2 "Cryptographic techniques based on elliptic curves – Part 2: Digital signatures"