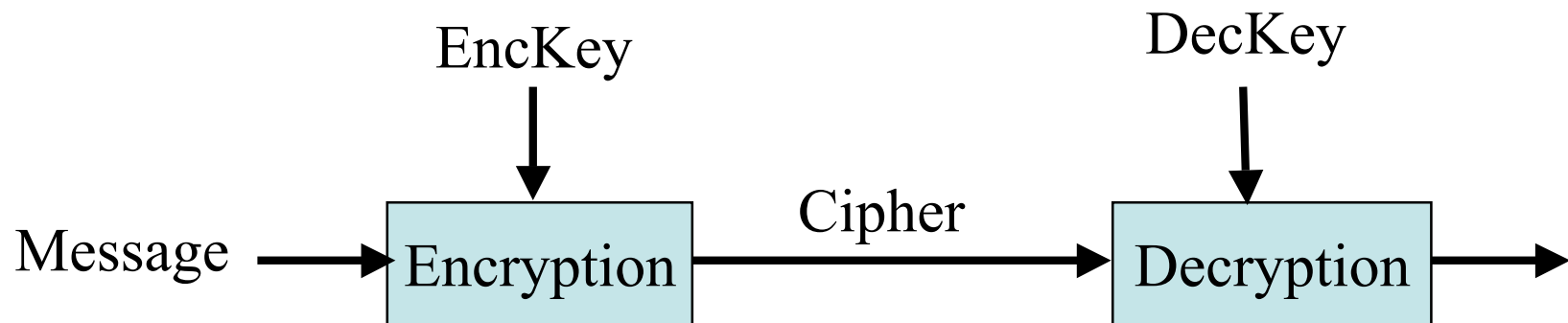


Risk in Cryptography
Damage Assessment for
Compromise of Cryptosystems

Eiji Okamoto
University of Tsukuba

Problems in Cryptosystems

- Development and Spread of Cryptosystems Everywhere
- Compromise of Cryptosystems
 - Damage of the Compromise
 - Planning for the Compromise



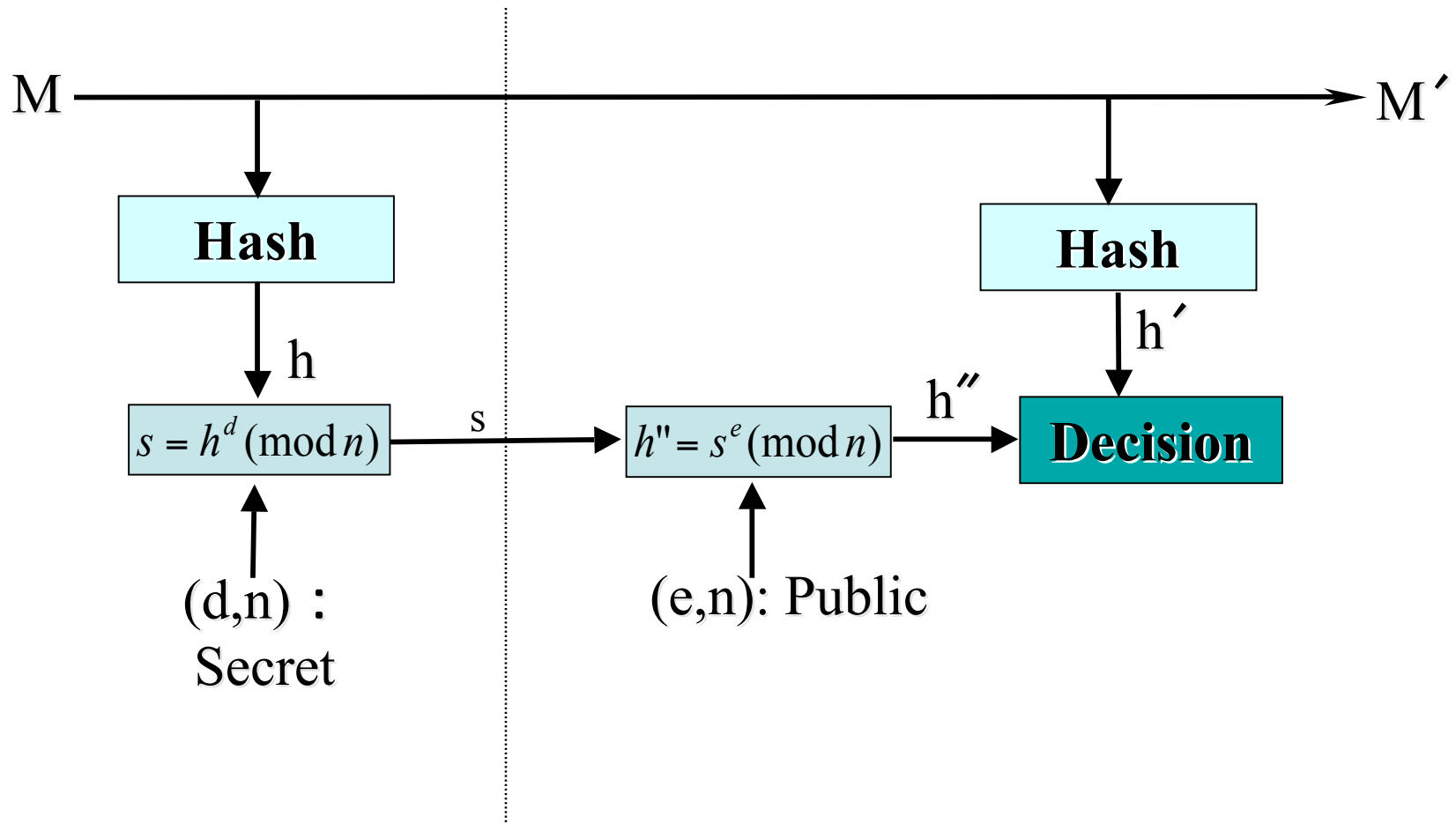
Break of Algorithm

- MD5 Collision
 - Xiaoyun Wang, Shandong University
Crypto Rump Session, Aug. 17, 2004
 - No more RIPEMD, MD4, MD5, SHA-0
 - Recommendation of SHA-256, SHA-512

Hash Function

- $hash(x)$ and $hash(y)$ are independent, even if x and y are related like $y=x+1$.
- Crucial Primitive to Guarantee the Security of Cryptosystems --- Random Oracle Model
 - Signature
 - Encryption: OAEP
- Pseudo Random Number Generators

RSA Sinature



NIST Response

- NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1
 - SHA-1 is strong yet, but phase out by 2010
 - Recommendation of SHA-224, 256, 384, 512

CRYPTREC Response

- No serious influence to CRYPTREC List
 - SHA-0, RIPEMD, MD4, MD5, HAVAL-128: not included
 - RIPEMD-160, SHA-1: noted “it is preferable that a 256-bit (or more) hash function be selected”
 - SHA-256, SHA-384, SHA-512

CRYPTREC

Cryptography Research & Evaluation Committees

- To make lists of cryptographic techniques for the common security basis to the Japanese e-Government. The project was started in 2000
- To watch the security of schemes in the list

CRYPTREC LIST 1

- Public-key ciphers

- Signature

- DSA, ECDSA, RSASSA-PKCS1-v1.5, RSA-PSS

- Confidentiality

- RSA-OAEP, RSAES-PKCS1-v1.5

- Key agreement

- DH, ECDH, PSEC-KEM

CRYPTREC LIST 2

- Symmetric-key ciphers

- 64-bit block ciphers

CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3-key Triple DES

- 128-bit block ciphers

AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000

- Stream ciphers

MUGI, MULTI-S01, 128-bit RC4

CRYPTREC LIST 3

- Others

- Hash function

- RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512

- Pseudo-random number generator

- PRNG based SHA-1 in ANSI X9.42-2001 Annex C.1,

- PRNG based SHA-1 for general purpose in FIPS 186-2
Appendix 3.1

- PRNG based SHA-1 for general purpose in FIPS 186-2
revised Appendix 3.1

Compromise of Cryptosystems -1

- Break of Algorithms: Encryption, Signature, Hash Function
 - Tool Progress: Device, Computer and Network
 - Attacks
 - Differential & Linear Attacks: Security Criteria
 - Factorization, Discrete Logarithm: TWIRL -- unrealistic
 - Hash Collision: MD5 and others
 - Algebraic Attack: XSL -- not serious
 - Side Channel Attack --Timing Attack, Cache Attack, Power Consumption Attack and others ---Open SSL update
- CMVP (Cryptographic Module Validation Program),
CRYPTREC Project
- Quantum Computing: realization of a couple qubits yet

Cache Attack

- Information of cache hit / miss is used.
- AES, Misty1, Camellia --- in 20 days
- Available information?

No More Weakness in Crypto?

- Elliptic Curve
 - Discrete Logarithm: $Q=kP$ --- in sub-exponential time?

Chris Monico and his team

ECC_p -109: 10,000 computers, 18 months, 2002-11-06

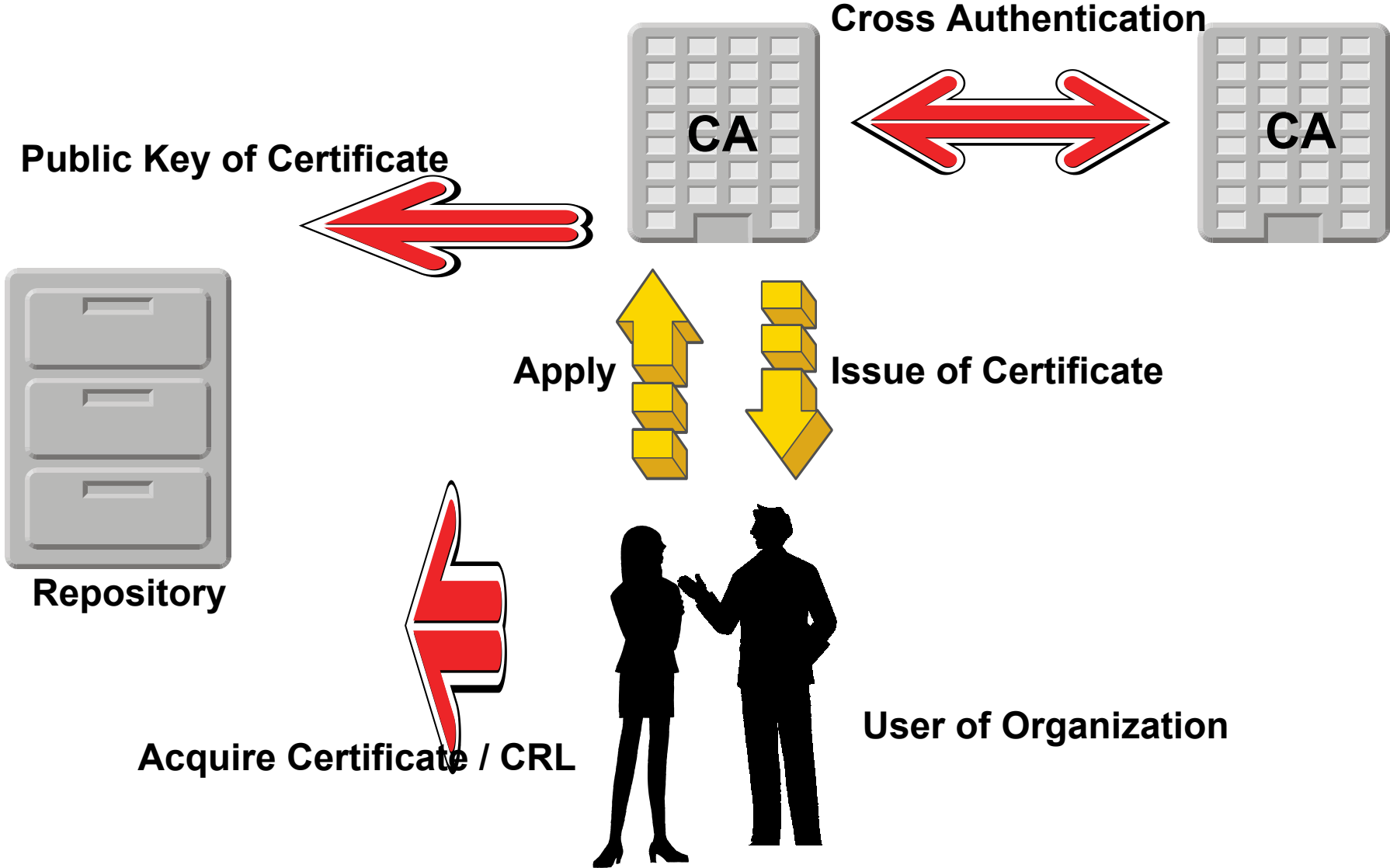
ECC_2 -109: 2600 computers, 17 months, 2004-04-27

- Pairing --- Many systems using the pairing, but secure more than 20 years?

Influence of Break of Algorithms

- To Infrastructure
 - PKI, Standardization
- To Applications
 - Consumer: Shopping, Voting, Auction...
 - Business: Medical Area, Banking, Government...
- Signature > Encryption
 - Loss of Credential/Trust > Loss of Confidentiality
 - Long Life > Short Life

PKI (Public Key Infrastructure)



Compromise of Cryptosystems - 2

- Leakage of Keys
(No Algorithm Break)
 - Internal Crime, Carelessness
 - Key Type: CA Key, User Key, Work Key
 - Similar influence by Algorithm Break, but limited
- Key Escrow System is useful for Key Loss, but not Key Leakage.

Compromise of Cryptosystems - 3

- Damage by Improper Introduction of Cryptosystems to Actual Business
 - Leakage of Privacy Information
 - Untrustness of Trusted Party
 - Uneasy Feeling about Cryptosystems among People

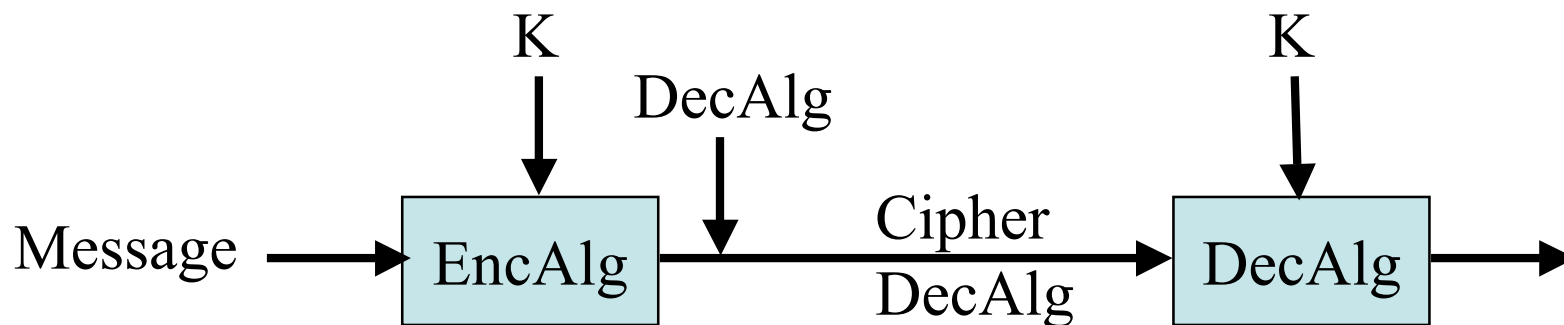
Planning for the Compromise

- Algorithms -

- Watching / Investigation System: Less Risk
 - Academic Research Community
 - Special Organization --- CRYPTREC, NIST
- Technical Methods
 - Short Life Message --- Not serious
 - Ex. Self-deciphering system / Renewal System / UC
 - Long Life Message --- Serious
 - Investigation on Management / Legal Approach by IPA
 - Composite Mechanism --- Signature + Hash Value Archive

Self-deciphering System

- Cipher Object:
 $C=[\text{Enc}(K, M) \mid \text{Decipher Algorithm}]$
- Flexibility against Algorithm Break, New Encryption Standard
- Server Type might be better, if the server updates frequently.



Planning for the Compromise

- Key Leakage -

- Certificate Revocation List
 - Inducing Complicated Work and Much Changes
- Some of the Planning for Algorithm Break might be useful --- Composite Mechanism
- Investigation of Key Leakage in PKI
 - To Evaluate the Damage of Leakage of Secret Key
 - Simulation of Damage to PKI
 - Time lag to recover
 - Undelivery case of certificate revocation list
 - Dependency on CRL structure

Thank you