# ID-based Cryptography and Smart-Cards

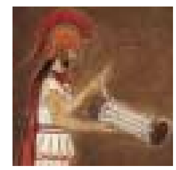
*Survol des techniques cryptographiques basées sur l'identité et implémentation sur carte à puce*

## The Need for Cryptography

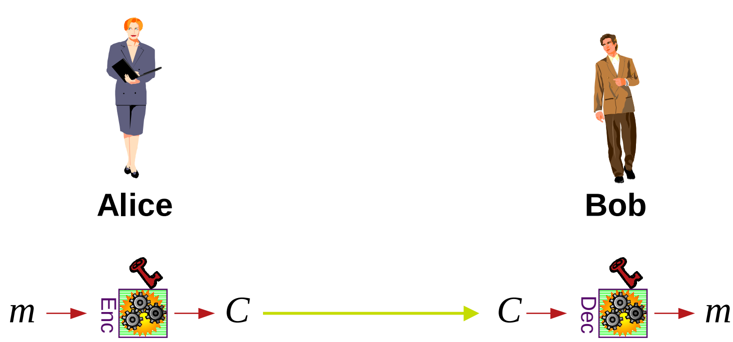
- Encryption
  - Transform a message so that only the intended recipient can read it
  - Privacy concerns
- Digital signature
  - Relate a message to an individual
  - Publicly verifiable and (computationally) impossible to forge
    - Non-repudiation

# Secret-Key Cryptography

- Cytale, Caesar, Vernam, DES, ...
  - Symmetric encryption



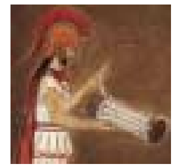
# Symmetric Encryption




Alice and Bob share the same key:

# Secret-Key Cryptography

- Cytale, Caesar, Vernam, DES, ...
  - Symmetric encryption



- Limitations
  - Number of keys: $n\,(n - 1)/2 \approx n^2$
  - Key distribution

GEMPLUS

# Public-Key Cryptography

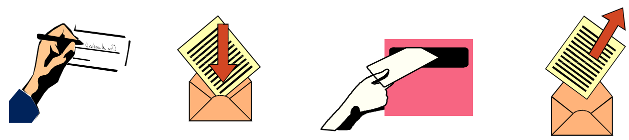
- Inventors
  - Whitfield Diffie
  - Martin Hellman
  - Ralph Merkle

- Publications
  - W. Diffie & M. Hellman, New directions in cryptography, IEEE TIT, 22 : 644-654, 1976
  - R. Merkle, Secure communications over insecure channels, CACM, 21: 294-299, 1978

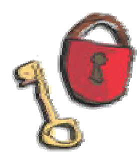
GEMPLUS

# Analogy

- Privacy
  - Exchange of encrypted mail

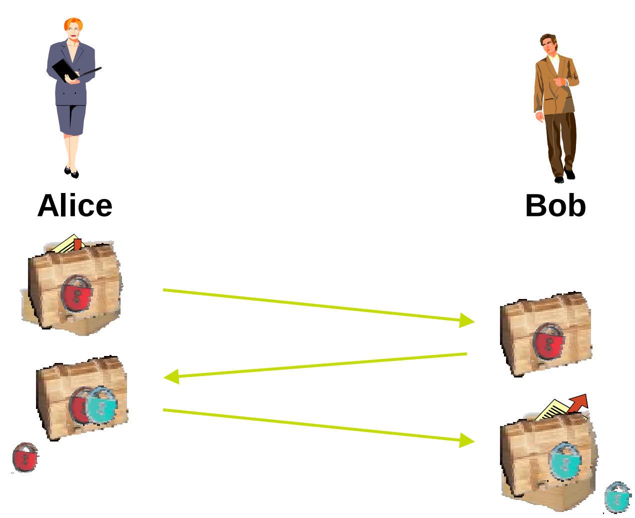


- Analogy to padlocked boxes



GEMPLUS

# Padlocked Boxes




Order is important

GEMPLUS

# Diffie-Hellman Key Exchange

**Alice**

? $x_A$

**Bob**

? $x_B$

$K_A = g^{x_A} \bmod p$ →

← $K_B = g^{x_B} \bmod p$

$K_{AB} = (K_B)^{x_A} \bmod p$

$K_{BA} = (K_A)^{x_B} \bmod p$

$K_{AB} = K_{BA}$

GEMPLUS

# Cryptographic Assumptions

- CDH problem
  - Given ($g^x \bmod p$, $g^y \bmod p$, $g$, $p$), compute $g^{xy} \bmod p$
- DL problem
  - Given ($g^x \bmod p$, $g$, $p$), compute $x$

GEMPLUS

# Public-Key Cryptosystems

- Diffie-Hellman allows to exchange a secret over an insecure channel

- Limitations
  - Delays
  - "*Man-in-the-middle*" attack

- Public-key cryptography
  - Asymmetric encryption
  - Exchange of encrypted mails (2)




# Rivest-Shamir-Adleman

- 3 M.I.T. researchers
  - Leonard Adleman
  - Ronald Rivest
  - Adi Shamir

- Publication
  - R. Rivest, A. Shamir & L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, CACM, 21 : 120-126, 1978

# RSA Cryptosystem (1/3)

- $\mathrm{Dec}_{SKB}(\mathrm{Enc}_{PKB}(m)) = m$
- Group $(\mathbb{Z}/N\mathbb{Z})^*$
  - Modular exponentiation in $(\mathbb{Z}/N\mathbb{Z})^*$
    - Permutation iff $\gcd(e, \phi(N)) = 1$
  - Euler theorem
- Security based on factoring $N$

GEMPLUS

# RSA Cryptosystem (2/3)

- Key generation (Bob)
  - $p_B$ et $q_B$, $N_B = p_B q_B$, $e_B$ s.t. $\gcd(e_B, \phi(N_B)) = 1$
  - $\mathrm{PK} = \{e_B, N_B\}$
  - $\mathrm{SK} = \{p_B, q_B, d_B\}$ with $d_B = e_B^{-1} \bmod \phi(N_B)$
- Encryption (Alice)
  - $C = m^{e_B} \bmod N_B$
- Decryption (Bob)
  - $C^{d_B} \bmod N_B$
- (Paddings)

GEMPLUS

# RSA Cryptosystem (3 / 3)

**Alice**

**Bob**

$e_B, N_B$ 

$C = m^{e_B} \bmod N_B$ →

$m = C^{d_B} \bmod N_B$

Bob's certificate needs to be verified

GEMPLUS

# Other Applications

- RSA signature (1978)
  - Based on factoring
  - Dual function of RSA encryption
- ElGamal encryption/signature (1985)
  - Based on DL
  - Other groups (e.g., elliptic curves)

GEMPLUS

# Identity-Based Cryptography

- Inventor
  - Adi Shamir, 1984

- Key idea
  - Identity serves as public-key
  - Certificates become implicit (inside a domain)
- No known solution for encryption

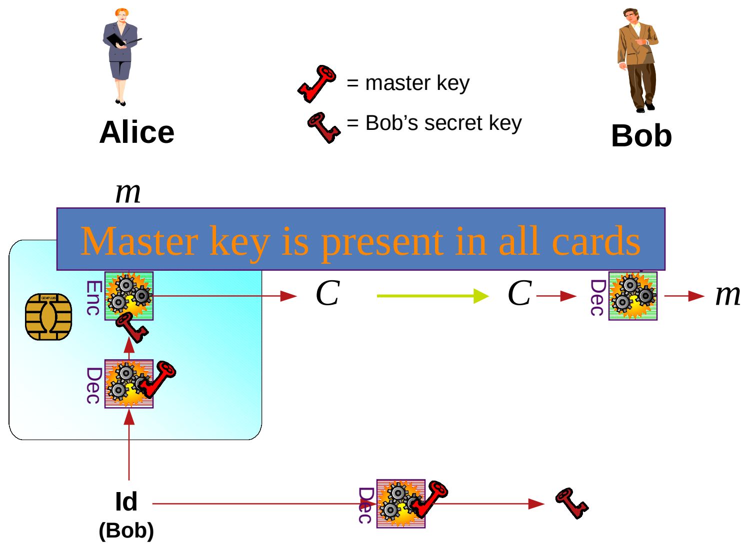


# Indentity-Based Encryption (1/2)

- Y. Desmedt and J.-J. Quisquater, 1986

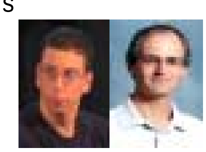
- Security assumptions
  - Enc(Dec($m$)) = $m$
  - Enc ≠ Dec
  - Tamper resistance

# Identity-Based Encryption (2/2)




# Boneh-Franklin

- Stanford/UC Davis researchers
  - Dan Boneh
  - Matt Franklin



- Publication
  - D. Boneh & M. Franklin, Identity based encryption from the Weil pairing, SIAM J. on Computing 32:586-615, 2003

## Boneh-Franklin IBE (1/3)

- $\mathrm{Dec}_{SKB}(\mathrm{Enc}_{IDB}(m)) = m$
- Admissible bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, i.e.,
  - [bilinear] $e(aP, bQ) = e(P, Q)^{ab}$
  - [non-degenerate] $e(P, P) \neq 1$
  - [computable] efficient algorithm for $e$
- Security based on BDH problem
  - Given $(P, aP, bP, cP)$, compute $e(P, P)^{abc}$

GEMPLUS

## Boneh-Franklin IBE (2/3)

- Set-up (TTP)
  - $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, $h: \{0,1\}^* \to \mathbb{G}_1$, $H: \mathbb{G}_2 \to \{0,1\}^{|m|}$
  - master SK: $s$
  - PK = $\{P_{pub} = s\,P, P, e, h, H\}$
- Extract (TTP) — e.g., for Bob
  - $d_{IDB} = s\,Q_{IDB}$ where $Q_{IDB} = h(ID_B)$
- Encryption (Alice)
  - $Q_{IDB} = h(ID_B)$ and $g_{IDB} = e(Q_{IDB}, P_{pub})$
  - $(C_1, C_2) = (rP, m \oplus H(g_{IDB}{}^r))$
- Decryption (Bob)
  - $m = C_2 \oplus H(e(d_{IDB}, C_1))$

GEMPLUS

# Boneh-Franklin IBE (3/3)

**Alice**

**Bob**

Sytem parameters

$Q_{ID_B} = h(ID_B)$

$g_{ID_B} = e(Q_{ID_B}, P_{pub})$

$(C_1, C_2) = (rP, m \oplus H(g_{ID_B}{}^r))$ ⟶

$m = C_2 \oplus H(e(d_{ID_B}, C_1))$

Verification of certificates is *implicit* (inside the domain)



# Smart IBE

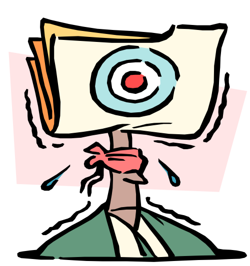
- Boneh-Franklin protocol on smart cards
- Prototype library
  - allowing to perform encryption/decryption
- First solution with the entire pairing computation performed on the smart card

# Summary & Perspectives

- State of the art
  - Symmetric encryption (3DES, AES)
  - Asymmetric encryption (RSA, ECC)
  - ID-based encryption (Boneh-Franklin IBE)
- Smart card solutions for ID-based encryption
  - Desmedt-Quisquater IBE
  - Boneh-Franklin IBE **(Smart IBE)**
- Future research
  - More efficient implementations of pairings on constrained devices
  - Share the master key *s* amongst several TTPs
  - Design an IBE based on "standard" assumptions

GEMPLUS

# Comments/Questions?



More info:

http://www.geocities.com/MarcJoye/

GEMPLUS