Joint Advanced Students Seminar 2005

The ElGamal Cryptosystem

Andreas V. Meier

meiera@in.tum.de

TUM Informatik

Structure

- Public Key Cryptography
- Assigned Complexity Problems
- ElGamal Cryptosystem
- Importance of Correct Implementation
- Summary

Public Key Cryptography

Introduced 1976 by Diffie and Hellman

Basic concept: Trapdoor functions (see following presentation)

Features:

- sender verification
- private key part remains at owner
- public key part freely distributable
- no secret channel neccessary
- no pre-shared keys

Prominent representative: RSA (1977) ... and ElGamal

Public Key Cryptography - Procedure

Scenario:

- Alice want's to send an encrypted message to Bob

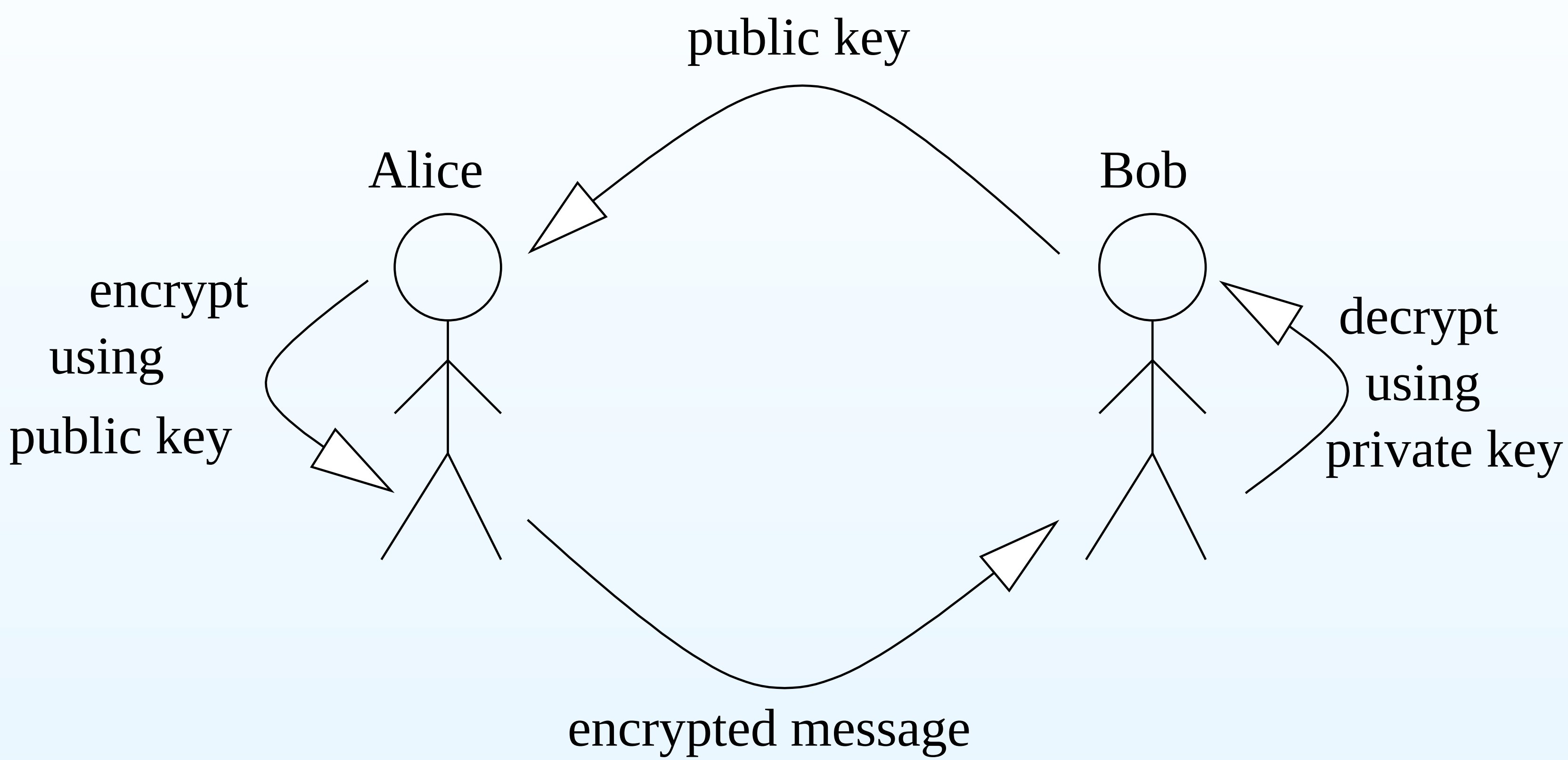
Procedure

1. Bob computes a public and a private key, the *keypair*
2. Bob publishes his public key
3. Alice Encrypts the message using Bob's public key
4. Alice sends the message to Bob.
5. Bob encrypts the message using his private key

Effect:

- Nobody intercepting the message can read
- nor alter it unrecognized

Public Key Cryptography - Scheme



Public Key Cryptography - Algorithm

Two public parameters:

- p: prime number
- g: generator such that $\forall n \in [1; p-1] : \exists k; n = g^k \bmod p$

Procedure:

1. - Alice generates a private random integer a
   - Bob generates a private random integer b
2. - Alice generates her public value $g^a \bmod p$
   - Bob generates his public value $g^b \bmod p$
3. - Alice computes $g^{ab} = (g^a)^b \bmod p$
   - Bob computes $g^{ba} = (g^b)^a \bmod p$
4. Both now have a shared secret k since $k = g^{ab} = g^{ba}$

Public Key Cryptography - Summary

Features

- able to set up a secure channel between two parties
- based on the Discrete Logarithm Problem

Problems

- vulnerable to the man-in-the-middle attack
- vulnerable to chosen-plaintext attacks ($\longrightarrow$ signed keys)
- not useful for one way communication (e.g. email)

Diffi e-Hellmann Problem – DH

Instance:

- A multiplicative group $(G, \cdot)$,
- a generator g of G,
- two public key parts g^a and g^b

Question:

- Find the common key g^{ab}

Discrete Logarithm Problem - DL

Instance:

- A multiplicative group $(G, \cdot)$,
- a generator g of G, $|G| = n$,
- and an element x

Question:

- Find the unique integer a, $0 \leq a \leq n-1$, such that $g^a = x$.
- a can be described as $\log_g x$

Complexity of DL and DH

Lower bound:

- $\Omega(\sqrt{p})$ with $p =$ greatest prime divisor of the group order

Related problem: Decision DH (DDH)

- Instance: the triple g^a, g^b and g^c
- Question: is $c \equiv ab \pmod{p}$?

Algorithms for DL

Given: Generator g of G, $beta \in G$

Wanted: a,$1 < a < p - 1$

Assumption: Multiplication of $x, y \in G$ in O(1)

1. compute all possible g^i into a list of pairs (i, g^i)
2. sort the list wrt. the second coordinate
3. given a β, perform a binary search on the list

First step: $O(n)$, Second step: $O(n \log n)$, Third step: $O(\log n)$

Neglecting logarithmic factors:
Precomputation-time: $O(1)$ Space: $O(n)$, Solving in $O(1)$

$\longrightarrow$ Shank, Pollard Rho, Pholig-Hellman

Complexity of DL - Reduction to Addition

So far we had a multiplicative Group $(G, *)$

Idea: DL in Additive Group $(G, +)$

ElGamal Cryptosystem

Presented in 1984 by Tather Elgamal

Key aspects:

- Based on the Discrete Logarithm problem
- Randomized encryption

Application:

- Establishing a secure channel for key sharing
- Encrypting messages

ElGamal Cryptosystem - Key Generation

Participant A generates the public/private key pair

1. Generate large prime p and generator g of the multiplicative Group $\mathbb{Z}_p^*$ pf of the integers modulo p.
2. Select a random integer a, $1 \leq a \leq p-2$, and compute $g^a \bmod p$.
3. A's Public key is (p, g, g^a); A's Private key is a.

ElGamal Cryptosystem - Encryption Procedure

Participant B encrypts a message m to A

1. Obtain A's authentic public key (p, g, g^a).
2. Represent the message as integers m in the range $\{0, 1, \ldots, p-1\}$.
3. Select a random integer k, $1 \leq k \leq p-2$.
4. Compute $\gamma = g^k \bmod p$ and $\delta = m * (g^a)^k$.
5. Send ciphertext $c = (\gamma, \delta)$ to A

ElGamal Cryptosystem - Decryption Procedure

Participant A receives encrypted message m from B

1. Use private key a to compute $(\gamma^{p-1-a}) \bmod p$.
   Note: $\gamma^{p-1-a} = \gamma^{-a} = a^{-ak}$
2. Recover m by computing $(\gamma^{-a}) * \delta \bmod p$.

ElGamal Cryptosystem - Encryption Sample

Alice choses her public key $(17, 6, 7)$:

- Prime $p = 17$
- Generator $g = 6$
- Private key part $a = 5$
- Public key part $g^a \bmod p = 6^5 \bmod 17 = 7$

Bob encrypts his message $m = 13$:

- He chooses a random $k = 10$
- He calculates $\gamma = g^k \bmod p = 6^{10} \bmod 17 = 15$
- He encrypts $\delta = m * g^k \bmod p = (13 * 7^{10}) \bmod 17 = 9$

Bob sends $\gamma = 15$ and $\delta = 9$ to Alice.

ElGamal Cryptosystem - Decryption Sample

Alice receives $\gamma = 15$ and $\delta = 9$ from Bob.

- Her public key is $(p, g, g^a) = (17, 6, 7)$
- Her private key is $a = 5$

Alice now decrypts the message using her private key:

- Decryption factor
  $(\gamma^{-a}) * \delta \mod p = 15^{-5} \mod 17 = 15^{11} \mod 17 = 9$
- Decryption: $(\delta * 9) \mod p = (9 * 9) \mod 17 = 13$

Alice has now decrypted the message and received: 13

ElGamal Cryptosystem - Summary

Features:

- use of a random factor k for encryption
- variant of DH: shared secret is g^{ak}

Problems:

- Duplicates message length
- Depends on intractability of DL and DH

Importance of Correct Implementation - GnuPG Issue

Problem discovered late 2003 by Phong Q. Nguyen in GnuPG

- Too small private exponent and
- too short nonce used for signature generation.
- Present for almost four years!

Effects

- All signatures created with GnuPG up to the day of fix considered compromised

Importance of Correct Implementation - Code Sample

```
/* IMO using a k much lesser than p is sufficient and it greatly
 * improves the encryption performance.  We use Wiener's table
 * and add a large safety margin.
 */
nbits = wiener_map( orig_nbits ) * 3 / 2;
nbytes = (nbits+7)/8;
```

Wiener Table:

$\|p\|$	512	768	1024	1280	1536	1792	2048	2304	...
q_{bit}	119	145	165	183	198	212	225	237	...

Small k in signature $\rightarrow$ lattice attack

Summary

What have we heared in this presentation?

- Public Key scheme - suitable for sharing symetric keys
- Discrete Logarithm Problem - even harder than $FACTORIZE$
- ElGamal Cryptosystem
- Importance of correct implementation of cryptosystems

Discussion

- Questions from the audience?
- Why are hybrid cryptosystems used for encrypting e.g. a vpn?

Literature

- *Cryptography: Theory and practice*, Douglas R. Stinson
- *New directions in cryptography*, Diffie and Hellman
- *Handbook of applied Cryptography*, Menezes, van Oorschot, Vanstone
- *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, Tather Elgamal