

UNIVERSITY OF MASSACHUSETTS
Dept. of Electrical & Computer Engineering

Introduction to Cryptography
ECE 597XX/697XX

Part 8

**Public-Key Cryptosystems Based on the Discrete
Logarithm Problem**

Israel Koren

ECE597/697 Koren Part.8 .1

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Content of this Chapter

- Diffie-Hellman Key Exchange
- The Discrete Logarithm Problem
- Security of the Diffie-Hellman Key Exchange
- The ElGamal Encryption Scheme

ECE597/697 Koren Part.8 .2

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Diffie-Hellman Key Exchange: Overview

- Proposed in 1976 by Diffie and Hellman
- Widely used, e.g. in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec)
- The Diffie-Hellman Key Exchange (DHKE) is a key exchange protocol and not used for encryption
(For the purpose of encryption based on the DHKE, ElGamal can be used.)

Setup:

- Choose a large prime p .
- Choose an integer $\alpha \in \{2, 3, \dots, p-2\}$.
- Publish p and α .

ECE597/697 Koren Part.8 .3

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Diffie-Hellman Key Exchange

Alice

Bob

Choose random private key
 $k_{prA} = a \in \{1, 2, \dots, p-1\}$

Choose random private key
 $k_{prB} = b \in \{1, 2, \dots, p-1\}$

Compute corresponding
public key

$A \rightarrow$

$B \leftarrow$

Compute corresponding
public key

$$k_{pubA} = A = \alpha^a \mod p$$

$$k_{pubB} = B = \alpha^b \mod p$$

Compute common secret

Compute common secret

$$k_{AB} = B^a = (\alpha^a)^b \mod p$$

$$k_{AB} = A^b = (\alpha^b)^a \mod p$$

$$(\alpha^a)^b = (\alpha^b)^a \mod p$$

We can now use the joint key k_{AB}
for encryption, e.g., with AES

$$y = \text{AES}_{k_{AB}}(x)$$

$y \rightarrow$

$$x = \text{AES}_{k_{AB}}^{-1}(y)$$

ECE597/697 Koren Part.8 .4

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Diffie-Hellman Key Exchange: Example

Domain parameters $p=29$, $\alpha=2$

Alice

Bob

Choose random private key

$$k_{prA} = a = 5$$

Choose random private key

$$k_{prB} = b = 12$$

Compute corresponding
public key

$$k_{pubA} = A = 2^5 = 3 \bmod 29$$

$$A=3$$



$$B=7$$



Compute corresponding
public key

$$k_{pubB} = B = 2^{12} = 7 \bmod 29$$

Compute common secret

$$k_{AB} = B^a = 7^5 = 16 \bmod 29$$

Compute common secret

$$k_{AB} = A^b = 3^{12} = 16 \bmod 29$$

Alice and Bob compute the same key k_{AB}

p is large so k_{AB} is large too

Use the 128 MSBs (for AES) or hash to 128 bits

ECE597/697 Koren Part.8 .5

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

The Discrete Logarithm (DLP) Problem in Z_p^*

Given: finite cyclic group Z_p^* of order $p-1$ and a primitive element $\alpha \in Z_p^*$ and another element $\beta \in Z_p^*$.

- The DLP is the problem of determining the integer $1 \leq x \leq p-1$ such that $\alpha^x \equiv \beta \bmod p$
- **DLP:** find $x = \log_\alpha \beta \bmod p$
- Example: Compute x for $5^x \equiv 41 \bmod 47$

- $5^{46} \equiv 1 \bmod 47$
- $\text{Ord}(5)=46$
- $12^{46} \equiv 1 \bmod 47$
- $\text{Ord}(12)=46$

ECE597/697 Koren Part.8 .6

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Cyclic groups and primitive elements

- * The group $Z_p^* = \{0, 1, \dots, p-1\}$ for p prime is commutative under multiplication mod p
- * The order of an element α , $\text{ord}(\alpha)$, of a group with the operation $\circ$ is the smallest integer k such that $\alpha^k = \underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{k \text{ times}} = 1 \text{ mod } p$

- Example: $a=3$ in Z_{11}^*

$$\begin{aligned} a^1 &= 3 \\ a^2 &= a \cdot a = 3 \cdot 3 = 9 \\ a^3 &= a^2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \text{ mod } 11 \\ a^4 &= a^3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \text{ mod } 11 \\ a^5 &= a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \text{ mod } 11 \end{aligned}$$
- $\text{Ord}(3)=5$

- The **cardinality** $|G|$ of the group $G=Z_p^*$ is the number of elements in G such that $\gcd(i,p)=1$, i.e., $|G|=\Phi(p)=p-1$
- A group G that contains an element α such that $\text{ord}(\alpha)=|G|$ (cardinality of G) is called **cyclic**; such α is called a **primitive element** (or **generator**) of G

- Example: $a=2$ in Z_{11}^*

$$\begin{aligned} a &= 2 & a^6 &\equiv 9 \text{ mod } 11 \\ a^2 &= 4 & a^7 &\equiv 7 \text{ mod } 11 \\ a^3 &= 8 & a^8 &\equiv 3 \text{ mod } 11 \\ a^4 &\equiv 5 \text{ mod } 11 & a^9 &\equiv 6 \text{ mod } 11 \\ a^5 &\equiv 10 \text{ mod } 11 & a^{10} &\equiv 1 \text{ mod } 11 \end{aligned}$$
- $\text{Ord}(2)=10$
- All elements of Z_{11}^* are generated

ECE597/697 Koren Part.8.7

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Cyclic groups and primitive elements

- For every element a in a cyclic group G , $\text{ord}(a)$ divides $|G|$ and $a^{|G|}=1$

$$\begin{array}{ll} \text{ord}(1) = 1 & \text{ord}(6) = 10 \\ \text{ord}(2) = 10 & \text{ord}(7) = 10 \\ \text{ord}(3) = 5 & \text{ord}(8) = 10 \\ \text{ord}(4) = 5 & \text{ord}(9) = 5 \\ \text{ord}(5) = 5 & \text{ord}(10) = 2 \end{array}$$
- Example: Z_{11}^*
- The number of primitive elements in G is $\Phi(|G|)$
- Example: for Z_{11}^* $\Phi(10)=(5-1)(2-1)=4$
- If $|G|$ is prime all elements $a \neq 1$ are primitive

ECE597/697 Koren Part.8.8

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

The Generalized Discrete Logarithm Problem

- Given a finite cyclic group G with the operation $\circ$ and cardinality $p-1$, consider a primitive element $\alpha \in G$ and another element $\beta \in G$.
- The discrete logarithm problem is finding the integer x , where $1 \leq x \leq p-1$, such that:

$$\beta = \underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{x \text{ times}} = \alpha^x \text{ mod } p$$

Two discrete logarithm problems are used in cryptography

1. The multiplicative group of the prime field Z_p or a subgroup of it, e.g., the classical DHKE, ElGamal encryption and the Digital Signature Algorithm (DSA).
2. The cyclic group formed by an elliptic curve (see Chapter 9)

ECE597/697 Koren Part.8 .9

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Attacks against the Discrete Logarithm

- Security of many asymmetric primitives is based on the difficulty of computing the DLP in cyclic groups, i.e., Compute x for a given α and β such that $\beta = \alpha \circ \alpha \circ \dots \circ \alpha = \alpha^x$
- The following algorithms for computing discrete logarithms exist
 - Generic algorithms: Work for any cyclic group
 - Brute-Force Search
 - Shanks' Baby-Step-Giant-Step Method
 - Pollard's Rho Method – Pohlig-Hellman Method
 - Non-generic Algorithms: Work only for specific groups, in particular in Z_p : The Index Calculus Method
- Elliptic curves can only be attacked with generic algorithms which are weaker than non-generic algorithms. Hence, elliptic curves are secure with shorter key lengths than the DLP in prime fields Z_p

ECE597/697 Koren Part.8 .10

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Attacks against the Discrete Logarithm Problem

Summary of records for computing discrete logarithms in $\mathbb{Z}_p^*$

Decimal digits	Bit length	Date
58	193	1991
68	216	1996
85	282	1998
100	332	1999
120	399	2001
135	448	2006
160	532	2007

To prevent attacks that compute the DLP, it is recommended to use primes with a length of at least 1024 bits for schemes such as Diffie-Hellman in $\mathbb{Z}_p^*$

ECE597/697 Koren Part.8 .11

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Security of the classical DH Key Exchange

- Which information does Oscar have?
 - α, p
 - $k_{pubA} = A = \alpha^a \bmod p$
 - $k_{pubB} = B = \alpha^b \bmod p$
- Which information does Oscar want to have?
 - $k_{AB} = \alpha^{ba} = \alpha^{ab} \bmod p$
 - This is known as Diffie-Hellman Problem (DHP)
- The only known way to solve the DHP is to solve the DLP, i.e.
 1. Compute $a = \log_{\alpha} A \bmod p$
 2. Compute $k_{AB} = B^a = \alpha^{ba} \bmod p$

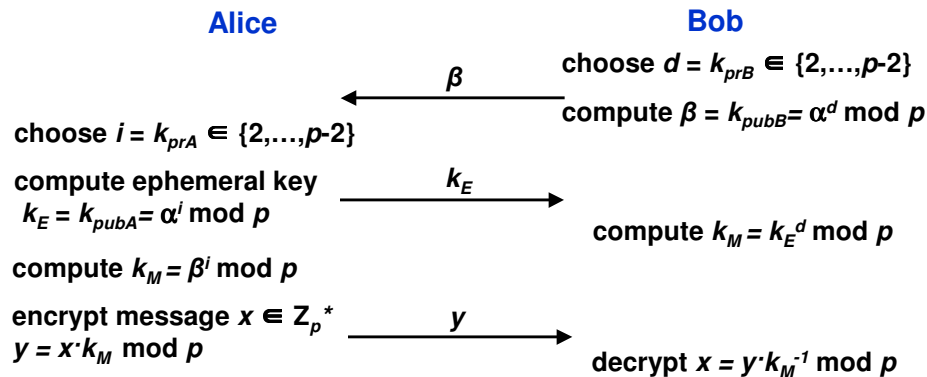
It is conjectured that the DHP and the DLP are equivalent, i.e., solving DHP implies solving DLP
- To prevent attacks, i.e., to prevent that the DLP can be solved, choose $p > 2^{1024}$

ECE597/697 Koren Part.8 .12

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

The ElGamal Encryption Scheme: Principle

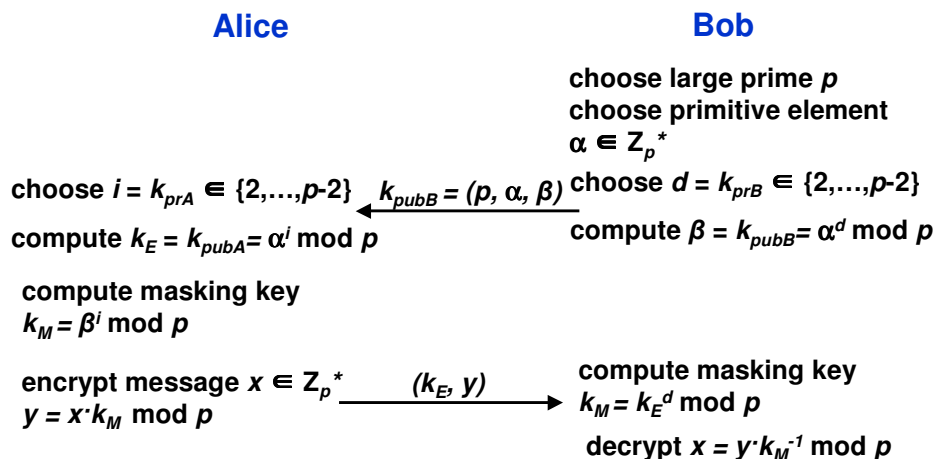
- Proposed by ElGamal in 1985 - can be viewed as an extension of the DHKE protocol
- Based on the intractability of the discrete logarithm and the Diffie-Hellman problems
- Select p and α



ECE597/697 Koren Part.8 .13

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

The ElGamal Encryption Protocol



The ElGamal protocol re-orders the computations to save one communication

ECE597/697 Koren Part.8 .14

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

The ElGamal Protocol - Example

Alice

Message $x=12$

choose $i = k_{prA} = 2$

$k_E = k_{pubA} = 3^2 = 9 \bmod 31$

masking key $k_M = 26^2 = 25 \bmod 31$

encrypt $x=12$:

$y = 12 \cdot 25 \bmod 31 = 21 \bmod 31$

$\gcd(31, 25) = \gcd(25, 6) = \gcd(6, 1) = 1$

$6 = 31 \cdot 1 - 25 \cdot 1$; $\{25 = 6 \cdot 4 + 1 = 31 \cdot 4 - 25 \cdot 4 + 1\}$

$\Rightarrow 1 = 25 \cdot 5 - 31 \cdot 4 \Rightarrow 25^{-1} = 5 \bmod 31$

Bob

$p=31$; primitive element $\alpha=3$

choose $d = k_{prB} = 5$

$\beta = k_{pubB} = \alpha^d = 3^5 = 26 \bmod 31$

$k_{pubB} = (31, 3, 26)$

masking key

$k_M = 9^5 = 25 \bmod 31$

decrypt $x = y \cdot k_M^{-1} \bmod p$

$= 21 \cdot 25^{-1} \bmod 31$

$= 21 \cdot 5 = 12 \bmod 31$

ECE597/697 Koren Part.8 .15

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Computational Aspects

- Key Generation
 - Generation of prime p : has to have at least 1024 bits
- Encryption
 - Requires two modular exponentiations and a modular multiplication
 - All operands have a bit length of $\log_2 p$
 - Efficient execution requires methods such as the square-and-multiply algorithm
- Decryption
 - Requires one modular exponentiation and one inversion
 - Inversion can be computed from the ephemeral key:

$$k_M^{-1} \bmod p = (k_E^d)^{-1} \bmod p = (k_E^d)^{-1} k_E^{p-1} \bmod p = k_E^{p-d-1} \bmod p$$

(Since $k_E^{p-1} = 1 \bmod p$ according to Fermat's little theorem)

Example: for $k_E=9$, $k_E^{p-d-1} \bmod p = 9^{31-5-1} = 9^{25} \bmod 31 = 5 \bmod 31$

ECE597/697 Koren Part.8 .16

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Security

- Passive attacks
 - Attacker eavesdrops p , α , $\beta = \alpha^d$, $k_E = \alpha^i$, $y = x \cdot \beta^i$ and wants to recover x
 - Problem relies on the DLP
- Active attacks
 - If the public keys are not authenticated, an attacker could send an incorrect public key (cf. Chapter 13)
 - An Attack is also possible if the secret exponent i is being used more than once (if you know/guess 1st message you can decrypt the 2nd)
 - ElGamal protocol is malleable: Oscar can replace (k_E, y) by $(k_E, s \cdot y)$ and the receiver would get $s \cdot x$

ECE597/697 Koren Part.8 .17

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Lessons Learned

- The Diffie-Hellman protocol is widely used for key exchange.
- The discrete logarithm problem is one of the most important one-way functions in modern asymmetric cryptography. Many public-key algorithms are based on it.
- For the Diffie-Hellman protocol in $\mathbb{Z}_p^*$, *the prime p should be at least 1024 bits long*. This provides a security roughly equivalent to an 80-bit symmetric cipher.
- For a better long-term security, a prime of length 2048 bits should be chosen.
- The ElGamal scheme is an extension of the DHKE where the derived **session key** is used as a multiplicative mask to encrypt a message.
- ElGamal is a probabilistic encryption scheme, i.e., encrypting two identical messages does not yield identical ciphertexts.

ECE597/697 Koren Part.8 .18

Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources