

# Introduction to Cryptography

## Lecture 6

Basic Number Theory,  
Diffie-Hellman Key Exchange

Benny Pinkas

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 1

## Last lecture

- Basic number theory
  - Integer numbers, divisors, primes
  - Modular operations
  - gcd algorithm
  - Extended gcd algorithm
    - Given  $a, b$  finds  $s, t$  such that  $\gcd(a, b) = a \cdot s + b \cdot t$
    - There is no common divisor smaller than  $\gcd(a, b)$  which can be represented as a linear combination of  $a, b$ 
      - For example,  $a=12, b=8$ .
      - $4 = 1 \cdot 12 - 1 \cdot 8$
      - There are no  $s, t$  for which  $2 = s \cdot 12 + t \cdot 8$

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 2

## Groups

- Definition: a set  $G$  with a binary operation  $\circ: G \times G \rightarrow G$  is called a group if:
  - (closure)  $\forall a, b \in G$ , it holds that  $a \circ b \in G$ .
  - (associativity)  $\forall a, b, c \in G$ ,  $(a \circ b) \circ c = a \circ (b \circ c)$ .
  - (identity element)  $\exists e \in G$ , s.t.  $\forall a \in G$  it holds that  $a \circ e = a$ .
  - (inverse element)  $\forall a \in G \exists a^{-1} \in G$ , s.t.  $a \circ a^{-1} = e$ .
- A group is Abelian (commutative) if  $\forall a, b \in G$ , it holds that  $a \circ b = b \circ a$ .
- Examples:
  - Integers under addition
    - $(\mathbb{Z}, +) = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 3

## More examples of groups

- Addition modulo  $N$ 
  - $(G, \circ) = (\{0, 1, 2, \dots, N-1\}, +)$
- $\mathbb{Z}_p^*$  Multiplication modulo a prime number  $p$ 
  - $(G, \circ) = (\{1, 2, \dots, p-1\}, \times)$
  - E.g.,  $\mathbb{Z}_7^* = (\{1, 2, 3, 4, 5, 6\}, \times)$
- Trivial: closure (the result of the multiplication is never divisible by  $p$ ), associativity, existence of identity element.
- The extended GCD algorithm shows that an inverse always exists:
  - $s \cdot a + t \cdot p = 1 \Rightarrow s \cdot a = 1 - t \cdot p \Rightarrow s \cdot a \equiv 1 \pmod{p}$

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 4

## More examples of groups

- $Z_N^*$  Multiplication modulo a composite number  $N$ 
  - $(G, \circ) = (\{a \text{ s.t. } 1 \leq a \leq N-1 \text{ and } \gcd(a, N)=1\}, \times)$
  - E.g.,  $Z_{10}^* = (\{1, 3, 7, 9\}, \times)$
  - Closure:
    - $s \cdot a + t \cdot N = 1$
    - $s' \cdot b + t' \cdot N = 1$
    - $ss' \cdot (ab) + (sat' + s'bt + tt'N) \cdot N = 1$
    - Therefore  $1 = \gcd(ab, N)$ .
  - Associativity: trivial
  - Existence of identity element: 1.
  - Inverse element: as in  $Z_p^*$

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 5

## Subgroups

- Let  $(G, \circ)$  be a group.
  - $(H, \circ)$  is a subgroup of  $G$  if
    - $(H, \circ)$  is a group
    - $H \subseteq G$
  - For example,  $H = (\{1, 2, 4\}, \times)$  is a subgroup of  $Z_7^*$ .
- *Lagrange's theorem:*  
If  $(G, \circ)$  is finite and  $(H, \circ)$  is a subgroup of  $(G, \circ)$ , then  $|H|$  divides  $|G|$

For example:  $3|6$ .

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 6

## Cyclic Groups

- Exponentiation is repeated application of  $\circ$ 
  - $a^3 = a \circ a \circ a$ .
  - $a^0 = 1$ .
  - $a^{-x} = (a^{-1})^x$
- A group  $G$  is cyclic if there exists a generator  $g$ , s.t.  
 $\forall a \in G, \exists i \text{ s.t. } g^i = a$ .
  - I.e.,  $G = \langle g \rangle = \{1, g, g^2, g^3, \dots\}$
  - For example  $Z_7^* = \langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$
- Not all  $a \in G$  are generators of  $G$ , but they all generate a subgroup of  $G$ .
  - E.g. 2 is not a generator of  $Z_7^*$
- The order of a group element  $a$  is the smallest  $j > 0$  s.t.  $a^j = 1$
- *Lagrange's theorem*  $\Rightarrow$  for  $x \in Z_p^*$ ,  $\text{ord}(x) \mid p-1$ .

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 7

## Fermat's theorem

- Corollary of Lagrange's theorem: if  $(G, \circ)$  is a finite group, then  $\forall a \in G, a^{|G|} = 1$ .
- Corollary (Fermat's theorem):  $\forall a \in Z_p^*, a^{p-1} = 1 \pmod p$ .  
E.g., for all  $\forall a \in Z_7^*, a^6 = 1, a^7 = a$ .
- Computing inverses:
- Given  $a \in G$ , how to compute  $a^{-1}$ ?
  - Fermat's theorem:  $a^{-1} = a^{|G|-1} (= a^{p-2} \text{ in } Z_p^*)$
  - Or, using the extended gcd algorithm (for  $Z_p^*$  or  $Z_N^*$ ):
    - $\gcd(a, p) = 1$
    - $s \cdot a + t \cdot p = 1 \Rightarrow s \cdot a = -t \cdot p + 1 \Rightarrow s$  is  $a^{-1} !!$
  - Which is more efficient?

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 8

## Computing in $Z_p^*$

- $P$  is a huge prime (1024 bits)
- Easy tasks (measured in bit operations):
  - Adding in  $O(\log p)$  (linear in the length of  $p$ )
  - Multiplying in  $O(\log^2 p)$  (and even in  $O(\log^{1.7} p)$ )
  - Inverting ( $a$  to  $a^{-1}$ ) in  $O(\log^2 p)$
  - Exponentiations:
    - $x^r \bmod p$  in  $O(\log r \cdot \log^2 p)$ , using repeated squaring

## Groups we will use

- $Z_p^*$  Multiplication modulo a prime number  $p$ 
  - $(G, \circ) = (\{1, 2, \dots, p-1\}, \times)$
  - E.g.,  $Z_7^* = (\{1, 2, 3, 4, 5, 6\}, \times)$
- $Z_N^*$  Multiplication modulo a composite number  $N$ 
  - $(G, \circ) = (\{a \text{ s.t. } 1 \leq a \leq N-1 \text{ and } \gcd(a, N)=1\}, \times)$
  - E.g.,  $Z_{10}^* = (\{1, 3, 7, 9\}, \times)$
- A group  $G$  is cyclic if there exists a generator  $g$ , s.t.
  - $\forall a \in G, \exists i \text{ s.t. } g^i = a.$
  - I.e.,  $G = \langle g \rangle = \{1, g, g^2, g^3, \dots\}$
  - For example  $Z_7^* = \langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$

## Euler's phi function

- Lagrange's Theorem:  $\forall a$  in a finite group  $G$ ,  $a^{|G|} = 1$ .
- Euler's phi function (aka, Euler's totient function),
  - $\phi(n)$  = number of elements in  $Z_n^*$  (i.e.  $|\{x \mid \gcd(x, n)=1, 1 \leq x \leq n\}|$ )
  - $\phi(p) = p-1$  for a prime  $p$ .
  - $n = \prod_{i=1..k} p_i^{e(i)} \Rightarrow \phi(n) = n \cdot \prod_{i=1..k} (1 - 1/p_i)$
  - $\phi(p^2) = p(p-1)$  for a prime  $p$ .
  - $n = p \cdot q \Rightarrow \phi(n) = (p-1)(q-1)$
- Corollary:  $\forall a \in Z_n^*$  it holds that  $a^{\phi(n)} = 1 \bmod n$ 
  - For  $Z_p^*$  (prime  $p$ ),  $a^{p-1} = 1 \bmod p$  (Fermat's theorem).
  - For  $Z_n^*$  ( $n = p \cdot q$ ),  $a^{(p-1)(q-1)} = 1 \bmod n$

## Finding prime numbers

- Prime number theorem:  $\#\{\text{primes} \leq x\} \approx x / \ln x$  as  $x \rightarrow \infty$
- How can we find a random  $k$ -bit prime?
  - Choose  $x$  at random in  $\{2^k, \dots, 2^{k+1}-1\}$
  - Test if  $x$  is prime
    - (more on this later in the course)
- The probability of success is  $\approx 1/\ln(2^k) = O(1/k)$ .
- The expected number of trials is  $O(k)$ .

## Finding generators

- How can we find a generator of  $Z_p^*$ ?
- Can check whether  $\forall 1 \leq i \leq p-2 \quad a^i \neq 1 \quad \text{⊗}$
- We know that if  $a^i = 1 \bmod p$  then  $i \mid p-1$ .
- Therefore need to check only  $i$  for which  $i \mid p-1$ .
- Easy if we know the factorization of  $(p-1)$ 
  - For all  $a \in Z_p^*$ , the order of  $a$  divides  $(p-1)$
  - For every integer divisor  $b$  of  $(p-1)$ , check if  $a^b = 1 \bmod p$ .
  - If none of these checks succeeds, then  $a$  is a generator.
  - $a$  is a generator iff  $\text{ord}(a) = p-1$ .

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 13

## Finding prime numbers of the right form

- How can we know the factorization of  $p-1$
- Easy, for example, if  $p = 2q+1$ , and  $q$  is prime.
- How can we find a  $k$ -bit prime of this form?
  1. Search for a prime number  $q$  of length  $k-1$  bits. (Will be successful after about  $O(k)$  attempts.)
  2. Check if  $2q+1$  is prime.
  3. If not, go to step 1.

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 14

## Quadratic Residues

- The square root of  $x \in Z_p^*$  is  $y \in Z_p^*$  s.t.  $y^2 = x \bmod p$ .
- Examples:  $\text{sqrt}(2) \bmod 7 = 3$ ,  $\text{sqrt}(3) \bmod 7$  doesn't exist.
- How many square roots does  $x \in Z_p^*$  have?
  - If  $a$  and  $b$  are square roots of  $x$ , then  $x = a^2 = b^2 \bmod p$ . Therefore  $(a-b)(a+b) = 0 \bmod p$ . Therefore either  $a = b$  or  $a = -b \bmod p$ .
  - Therefore  $x$  has either 2 or 0 square roots, and is denoted as a Quadratic Residue (QR) or Non Quadratic Residue (NQR), respectively. How many QRs there are?
- $x^{(p-1)/2}$  is either 1 or -1 in  $Z_p^*$ . (indeed,  $(x^{(p-1)/2})^2$  is always 1)
- Euler's theorem:  $x \in Z_p^*$  is a QR iff  $x^{(p-1)/2} = 1 \bmod p$ .
- Legendre's symbol:
 
$$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ is a QR in } Z_p^* \\ -1 & x \text{ is an NQR in } Z_p^* \\ 0 & x = 0 \bmod p \end{cases}$$
- Can be efficiently computed as  $x^{(p-1)/2} \bmod p$ .

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 15

## Hard problems in cyclic groups

- The following problems are believed to be hard in  $Z_p^*$  or in some subgroups of  $Z_p^*$ 
  - Discrete logarithm: let  $g$  be a generator of  $G$ . The input is a random  $x \in G$ . The task is to find an  $r$  s.t.  $x = g^r \bmod p$ .
  - The Diffie-Hellman problem: The input contains  $g$  and random  $x, y \in G$ , such that  $x = g^a$  and  $y = g^b$ . The task is to find  $z = g^{a \cdot b}$ .
  - The Decisional Diffie-Hellman problem: The input contains random  $x, y \in G$ , such that  $x = g^a$  and  $y = g^b$ ; and a pair  $(z, z')$  where one of  $(z, z')$  is  $g^{a \cdot b}$  and the other is  $g^c$  (for a random  $c$ ). The task is to tell which of  $(z, z')$  is  $g^{a \cdot b}$ .
- Solving DDH  $\leq$  solving DH  $\leq$  solving DL
  - All believed to be hard if  $|p| > 1024$  (check the next slide)

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 16

## Does the DDH assumption hold in $Z_p^*$ ?

- The DDH assumption does not hold in  $Z_p^*$ 
  - Assume that both  $x=g^a$  and  $y=g^b$  are QRs in  $Z_p^*$ .
  - Namely, their Legendre symbol is 1, both  $a$  and  $b$  are even, and it holds that  $x^{(p-1)/2} = y^{(p-1)/2} = 1$ .
  - Then the Legendre symbol of  $g^{ab}$  is always 1, whereas the symbol of a random  $g^c$  is 1 with probability  $1/2$ .
- Solution: (work in a subgroup of prime order)
  - Set  $p=2q+1$ , where  $q$  is prime.
  - $\phi(Z_p^*) = p-1 = 2q$ . Therefore  $Z_p^*$  has a subgroup  $H$  of prime order  $q$ .
  - Let  $g$  be a generator of  $H$  (i.e.,  $g$  is a QR in  $Z_p^*$ ).
  - The DDH assumption is believed to hold in  $H$ . (The Legendre symbol is always 1.)

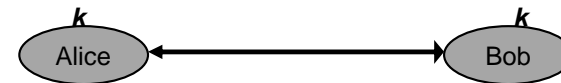
December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 17

## Classical symmetric ciphers

- Alice and Bob share a private key  $k$ .
- System is secure as long as  $k$  is secret.
- Major problem: generating and distributing  $k$ .



December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 18

## Diffie and Hellman: "New Directions in Cryptography", 1976.

- "We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing...
  - ...such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution...
  - ...theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science."

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 19

## Diffie-Hellman

- Came up with the idea of public key cryptography



Everyone can learn Bob's public key and encrypt messages to Bob. Only Bob knows the decryption key and can decrypt.

Key distribution is greatly simplified.

- Diffie and Hellman did not have an implementation for a public key encryption system
- Suggested a method for key exchange over insecure communication lines, that is still in use today.

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 20

## Public Key-Exchange

- Goal: Two parties who do not share any secret information, perform a protocol and derive the same shared key.
- No eavesdropper can obtain the new shared key (if it has limited computational resources).
- The parties can therefore safely use the key as an encryption key.

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 21

## The Diffie-Hellman Key Exchange Protocol

- Public parameters: a group  $Z_p^*$  (where  $|p|= 768$  or  $1024$ ,  $p=2q+1$ ), and a generator  $g$  of  $H \subset Z_p^*$  of order  $q$ .
- Alice:
  - picks a random  $a \in [1, q]$ .
  - Sends  $g^a \bmod p$  to Bob.
  - Computes  $k = (g^b)^a \bmod p$
- Bob:
  - picks a random  $b \in [1, q]$ .
  - Sends  $g^b \bmod p$  to Bob.
  - Computes  $k = (g^a)^b \bmod p$
- $K = g^{ab}$  is used as a shared key between Alice and Bob.
  - DDH assumption  $\Rightarrow K$  is indistinguishable from a random key

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 22

## Diffie-Hellman: security

- A (passive) adversary
  - Knows  $Z_p^*$ ,  $g$
  - Sees  $g^a$ ,  $g^b$
  - Wants to compute  $g^{ab}$ , or at least learn something about it
- Recall the Decisional Diffie-Hellman problem:
  - Given random  $x, y \in Z_p^*$ , such that  $x = g^a$  and  $y = g^b$ ; and a value  $z$  which is either  $g^{ab}$  or  $g^c$  (for a random  $c$ ), it is hard to tell which is the case.
  - I.e.,  $g^{ab}$  is indistinguishable from a random element in  $H$ .
  - Note: it is insufficient to require that the adversary cannot compute  $g^{ab}$ .

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 23

## Diffie-Hellman key exchange: usage

- The DH key exchange can be used in any group in which the Decisional Diffie-Hellman (DDH) assumption is believed to hold.
- Currently,  $Z_p^*$  and elliptic curve groups.
- Common usage:
  - Overhead: 1-2 exponentiations
  - Usually,
    - A DH key exchange for generating a master key
    - Master key used to encrypt session keys
    - Session key is used to encrypt traffic with a symmetric cryptosystem

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 24

## An active attack against the Diffie-Hellman Key Exchange Protocol

- An active adversary Eve.
- Can read and change the communication between Alice and Bob.
- ...As if Alice and Bob communicate via Eve.



December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 25

## Man-in-the-Middle: an active attack against the Diffie-Hellman Key Exchange protocol

- Alice:
    - picks a random  $a \in [1, q]$ .
    - Sends  $g^a \bmod p$  to Bob.
  - Bob:
    - picks a random  $b \in [1, q]$ .
    - Sends  $g^b \bmod p$  to Alice.
- Eve changes  $g^a$  to  $g^c$
- Eve changes  $g^b$  to  $g^d$
- Computes  $k = (g^d)^a \bmod p$
  - Computes  $k = (g^c)^b \bmod p$

Keys:

Alice	Eve	Bob
$g^{ad}$	$g^{ad}, g^{bc}$	$g^{bc}$

– Solution: ?

December 6, 2006

Introduction to Cryptography, Benny Pinkas

page 26