T-79.159
Cryptography and Data Security

Lecture 8:
- Finite fields and cyclic groups
- Discrete Logarithm Problem
- Diffie-Hellman key agreement scheme
- ElGamal public key encryption

Kaufman et al: Ch 6
Stallings: Ch 5, 8, 10

1

Axioms: Group

Group (G,∗): A set G, with operation ∗.

Additive group: "∗" is addition +

Multiplicative group: "∗" is multiplication ·

Axiom 1: G is closed under the operation ∗, that is, given a∈G and b∈G, then a∗b∈G.

Axiom 2: Operation ∗ is associative, that is, given a∈G,b∈G and c∈G, then (a∗b)∗c = a∗(b∗c).

Axiom 3: There is an identity element in (G,∗), that is, an element e∈G (identity element) such that a∗e = e∗a = a, for all a∈G. Then e is denoted by 1 (general and multiplicative case), or by 0 (additive case)

Axiom 4: Every element has an inverse, that is, given a∈G there is a unique b∈G such that a∗b = b∗a = e. Then b is denoted by a^{-1} (general or multiplicative case) or by –a (additive case).

2

Axioms: Abelian Group

Axiom 5: Group $(G,*)$ is Abelian group (or commutative group) if the operation $*$ is commutative, that is, given $a \in G$ and $b \in G$, then $a*b = b*a$.

3

Axioms: Ring $(R,+,\cdot)$

A set R with two operations + and $\cdot$ is a ring if the following eight axioms hold:

$\left.\begin{array}{l}\text{A1: Axiom 1 for +}\\ \text{A2: Axiom 2 for +}\\ \text{A3: Axiom 3 for +}\\ \text{A4: Axiom 4 for +}\\ \text{A5: Axiom 5 for +}\end{array}\right\}$ (R,+) is an Abelian Group

M1: Axiom 1 for $\cdot$

M2: Axiom 2 for $\cdot$

M3: Distributive laws hold, that is, given $a \in G, b \in G$ and $c \in G$, then $a\cdot(b+c) = a\cdot b+a\cdot c$ and $(a+b)\cdot c = a\cdot c+b\cdot c$.

4

Axioms: Commutative Ring and Field

A ring (R,+,·) is commutative if

M4: Axiom 5 for multiplication holds

A commutative ring (F,+,·) is a field if :

M5: Axiom 3 for · in F-{0}, that is, $a*1 = 1*a = a$, for all $a \in F$, $a \neq 0$.

M6: Axiom 4 for · in F-{0}, that is, given $a \in F$, $a \neq 0$, there is a unique $a^{-1} \in F$ such that $a * a^{-1} = a^{-1} * a = 1$.

If (F,+,·) is a field, then $F^* = F-\{0\}$ with multiplication is a group.

Example: p prime, then $Z_p = \{a \mid 0 \leq a < p\}$ with modulo p addition and multiplication is a field and $(Z_p^*, \cdot)$ is a group.

5

Polynomial Arithmetic

- Modular arithmetic with polynomials
- We limit to the case where polynomials have binary coefficients, that is, 1+1 = 0, and + is the same as -.

Example:

$$(x^2+x+1)(x^3+x+1) =$$
$$x^5+x^3+x^2+x^4+x^2+x+x^3+x+1 =$$
$$x^5+x = x\cdot(x^4+1) = x\cdot x = x^2 (\mathrm{mod}(x^4+x+1))$$

Computation $\mathrm{mod}(x^4+x+1)$ means that everywhere we take $x^4+x+1=0$,which means, for example, that $x^4+1=x.$

6

Galois Field

Given a binary polynomial f(x) of degree n, consider a set of binary polynomials with degree less than n. This set has 2^n polynomials. With polynomial arithmetic modulo f(x) this set is a ring.

Faxt: If f(x) is irreducible, then this set with 2-ary (binary) polynomial arithmetic is a field denoted by $GF(2^n)$.

In particular, every nonzero polynomial has a multiplicative inverse modulo f(x). We can compute a multiplicative inverse of a polynomial using the Extended Euclidean Algorithm.

Example: Compute the multiplicative inverse of x^2 modulo $x^4 + x + 1$

7

Extended Euclidean Algorithm for polynomials Example

i	q_i	r_i	u_i	v_i
-2		$x^4 + x + 1$	0	1
-1		x^2	1	0
0	x^2	$x+1$	x^2	1
1	x	x	x^3+1	x
2	1	1	x^3+x^2+1	$x+1$

8

Extended Euclidean Algorithm for polynomials Example cont'd

So we get

$u_2 \cdot x^2 + v_2 \cdot (x^4 + x + 1) = (x^3 + x^2 + 1)x^2 + (x+1)(x^4 + x + 1)$

from where the multiplicative inverse of x^2 modulo $x^4 + x + 1$ is equal to $x^3 + x^2 + 1$.

Motivation for polynomial arithmetic:

- uses all n-bit numbers
- provides uniform distribution of the multiplication result

9

Example: Modulo 2^3 arithmetic compared to $GF(2^3)$ arithmetic (multiplication).

In $GF(2^n)$ arithmetic, we identify polynomials of degree less than n:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

with bit strings of length n: $(a_0, a_1, a_2, \ldots, a_{n-1})$

and further with integers less than 2^n:

$$a_0 + a_1 2 + a_2 2^2 + \cdots + a_{n-1} 2^{n-1}$$

Example: In $GF(2^3)$ arithmetic with polynomial x^3+x+1 (see next slide) we get:

$4 \cdot 3 = (100) \cdot (011) = x^2 \cdot (x+1) = x^3 + x^2 = (x+1) + x^2 = x^2 + x + 1 = (111) = 7$

10

Multiplication tables

modulo 8 arithmetic

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$GF(2^3)$ Polynomial arithmetic

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	6
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

11

Generated set

Example: Finite field Z_{19}

$g = 7$

$g^i \bmod 19$

i	g^i
0	1
1	7
2	49=11
3	77=1
4	7
5	11
…	…

12

Generated elements

Example: Finite field Z_{19}

$g = 2$
$g^i \bmod 19$, $i = 0,1,2,\ldots$

Element $a = 2$ generates all nonzero elements in Z_{19}. Such an element is called primitive.

i	g^i
0	1
1	2
2	4
3	8
4	16
5	13
6	7
7	14
8	9
9	18

i	g^i
10	17
11	15
12	11
13	3
14	6
15	12
16	5
17	10
18	1

13

Cyclic subgroups

F finite field, $g \in F^*$, let $\langle g \rangle$ denote the set generated by g; $\langle g \rangle = \{1=g^0,g^1,g^2,\ldots,g^{r-1}\}$, where r is the least positive number such that $g^r=1$ in F. By Fermat's and Euler's theorems $r \leq \# F^*$.

r is the order of g.

$\langle g \rangle$ is a subgroup of the multiplicative group F^* of F.

Axiom 1: $g^i \cdot g^j = g^{i+j} \in \langle g \rangle$.

Axiom 2: associativity is inherited from F

Axiom 3: $1 = g^0 \in \langle g \rangle$.

Axiom 4: Given $g^i \in \langle g \rangle$ the multiplicative inverse is g^{r-i}, as $g^i \cdot g^{r-i} = g^{r-i} \cdot g^i = g^r = 1$

$\langle g \rangle$ is called a cyclic group. The entire F^* is a cyclic group generated by a primitive element, e.g, $Z_{19}^* = \langle 2 \rangle$.

14

Example: Cyclic group in Galois Field

GF(2^4) with polynomial $f(x) = x^4 + x + 1$

$g = 0011 = x+1$
$g^2 = x^2+1=0101$
$g^3 = (x+1)(x^2+1) = x^3 + x^2 + x + 1 = 1111$
$g^4 = (x+1)(x^3 + x^2 + x + 1) = x^4 + 1 = x = 0010$
$g^5 = (x+1)(x^4 + 1) = x^5 + x^4 + x + 1 = x^2 + x = 0110$
$g^6 = (x+1)(x^2 + x) = x^3 + x = 1010$
$g^7 = (x+1)(x^3 + x) = x^4 + x^3 + x^2 + x = x^3 + x^2 +1= 1101$
$g^8 = (x+1)(x^3 + x^2 +1) = x^4 + x^2 +x+1= x^2 =0100$
$g^9 = (x+1)x^2 = x^3 + x^2 = 1100$
$g^{10} = (x+1)(x^3 + x^2)= x^2 + x + 1= 0111$
$g^{11} = (x+1)(x^2 + x +1) = x^3 + 1 = 1001$
$g^{12} = (x+1)(x^3 + 1) = x^3 = 1000$
$g^{13} = (x+1)x^3 = x^3 + x + 1 = 1011$
$g^{14} = (x+1)(x^3 + x + 1) = x^3 + x^2 +x = 1110$
$g^{15} = (x+1)(x^3 + x^2 +x) = 1= 0001$

Discrete logarithm

Given $a \in \langle g \rangle = \{1,g^1,g^2,\ldots,g^{r-1}\}$, there is x, $0 \leq x < r$ such that $a = g^x$. The exponent x is called the discrete logarithm of a to the base g.

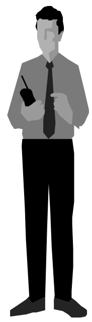
Example: Solve the equation

$$2^x = 14 \bmod 19$$

We find the solution using the table (slide 13): x =7.

Without the precomputed table the discrete logarithm is often hard to solve. Cyclic groups, where the discrete logarithm problem is hard, are used in cryptography.

Diffie-Hellman Key Exchange

ALICE		BOB
 a secret $A = g^{\mathbf{a}} \mod p$		b secret $B = g^{\mathbf{b}} \mod p$ 
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
$K = B^{\mathbf{a}} \mod p$		$K = A^{\mathbf{b}} \mod p$

17

Security of Diffie-Hellman Key Exchange

- If the Discrete Logarithm Problem (DLP) is easy then DH KE is insecure
- Diffie-Hellman Problem (DHP):

  Given g, g^a, g^b, compute g^{ab}.
- It seems that in groups where the DHP is easy, also the DL is easy. It is unknown if this holds in general.
- DH KE is secure against passive wiretapping.
- DH KE is insecure under the active man-in-the-middle attack: Man-in-the-Middle exchanges a secret key with Alice, and another with Bob, while Alice believes that she is talking confidentially to Bob, and Bob believes he is talking confidentially to Alice (see next slide).
- This problem is solved by authenticating the Diffie-Hellman key exchange messages.

18

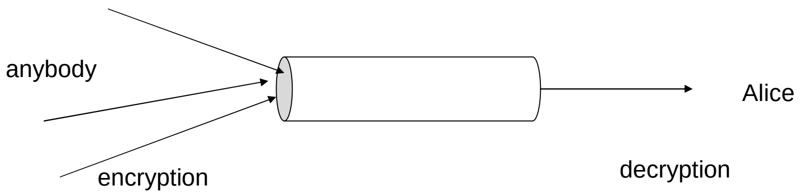
Man-in-the-Middle in the DH KE

Alice		Carl (man-in-the-middle)		Bob
a		$c1$		
g^a	$g^a \longrightarrow$	g^{c1}	$g^{c1} \longrightarrow$	b
			$\longleftarrow g^b$	g^b
		$c2$		
	$\longleftarrow g^{c2}$	g^{c2}		
$K_2= (g^a)^{c2}$		$K_1= (g^b)^{c1}$		$K_1= (g^b)^{c1}$
		$K_2= (g^a)^{c2}$		
	Protection using K_2 $\longleftrightarrow$		Protection using K_1 $\longleftrightarrow$	

19

Recall: The Principle of Public Key Cryptosystems

Encryption operation is public
Decryption is private



Alice's key for a public key cryptosystem is a pair: (K_{pub},K_{priv}) where K_{pub} is public and K_{priv} is cannot be used by anybody else than Alice.

20

Setting up the ElGamal public key cryptosystem

- Alice selects a primitive element g in Z_p^* .
- Alice generates a, 0< a < p-1, and computes g^a mod p = A.
- Alice's public key: K_{pub} = (g, A)
- Alice's private key: K_{priv} = a
- Encryption of message m $\in$ Z_p^* : Bob generates a secret, unpredictable k, 0< k < p-1. The encrypted message is the pair (g^kmod p, ($A^k \cdot$m) mod p).
- Decryption of the ciphertext: Alice computes $(g^{k)a}= A^k$ mod p, and the multiplicative inverse of A^k mod p. Then m = $(A^k)^{-1} \cdot$ ($A^k \cdot$m) mod p.

Diffie-Hellman Key Exchange and ElGamal Cryptosystem can be generalised to any cyclic group, where the discrete logarithm problem is hard.

21