T-79.4501
Cryptography and Data Security

Lecture 8:

- Discrete Logarithm Problem
- Diffie-Hellman key agreement scheme
- ElGamal public key encryption

Stallings: Ch 5, 8, 10

Cyclic multiplicative group of finite field

Given a finite field $\mathbf{F}$ with q elements and an element $g \in \mathbf{F}$ consider a subset in $\mathbf{F}$ formed by the powers of g:

$$\{g^0 = 1, g, g^2, g^3, \ldots\}$$

Since $\mathbf{F}$ is finite, this set must be finite. Hence there is a number r such that $g^r = 1$. By Fermat's theorem, one such number is $q - 1$. Let r be the smallest number with $g^r = 1$. Then r divides $q - 1$, and r is called the *order* of g. The set

$$\{g, g^2, g^3, \ldots, g^{r-1}, g^r = 1 = g^0\}$$

is called the cyclic group generated by g.

There are elements $\alpha \in \mathbf{F}$ such that $r = q - 1$ and

$$\{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\} = \mathbf{F} - \{0\} = \mathbf{F}^*$$

Such element α is called *primitive element* in $\mathbf{F}$.

Generated set of a primitive element

Example: Finite field $\mathbf{Z}_{19}$

$g = 2$

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

Element $g = 2$ generates all nonzero elements in $\mathbf{Z}_{19}$. It is a primitive element.

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

Cyclic subgroups

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

Definition*:* r is the order of g.

$<g>$ is a subgroup of the multiplicative group $\mathbf{F}^*$ in **F**.

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

Axiom 2: associativity is inherited from **F**

Axiom 3: $1 = g^0 \in <g>$.

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

$<g>$ is called a cyclic group. The entire $\mathbf{F}^*$ is a cyclic group generated by a primitive element, e.g, $\mathbf{Z}_{19}^* = <2>$.

Generated set of g

Example: Finite field $\mathbf{Z}_{19}$

$g = 7$

$g^{i} \bmod 19$

The multiplicative order of 7 is 3 in $\mathbf{Z}_{19}$.

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

Example: Cyclic group in Galois Field

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

$g = 0011 = x + 1$

$g^2 = x^2 + 1 = 0101$

$g^3 = (x+1)(x^2+1) = x^3 + x^2 + x + 1 = 1111$

$g^4 = (x+1)(x^3 + x^2 + x + 1) = x^4 + 1 = \mathrm{x} = 0010$

$g^5 = (x+1)(x^4 + 1) = x^5 + x^4 + x + 1 = x^2 + x = 0110$

$g^6 = (x+1)(x^2 + x) = x^3 + x = 1010$

$g^7 = (x+1)(x^3 + x) = x^4 + x^3 + x^2 + x = x^3 + x^2 + 1 = 1101$

$g^8 = (x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1 = x^2 = 0100$

$g^9 = (x+1)x^2 = x^3 + x^2 = 1100$

$g^{10} = (x+1)(x^3 + x^2) = x^2 + x + 1 = 0111$

$g^{11} = (x+1)(x^2 + x + 1) = x^3 + 1 = 1001$

$g^{12} = (x+1)(x^3 + 1) = x^3 = 1000$

$g^{13} = (x+1)x^3 = x^3 + x + 1 = 1011$

$g^{14} = (x+1)(x^3 + x + 1) = x^3 + x^2 + x = 1110$

$g^{15} = (x + 1)(x^3 + x^2 + x) = 1 = 0001$

Discrete logarithm

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

Example: Solve the equation

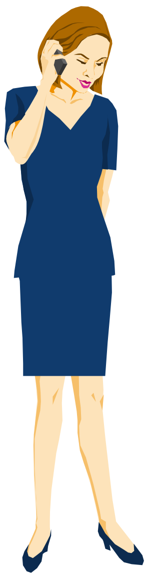
$$2^x = 14 \bmod 19$$

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



a secret

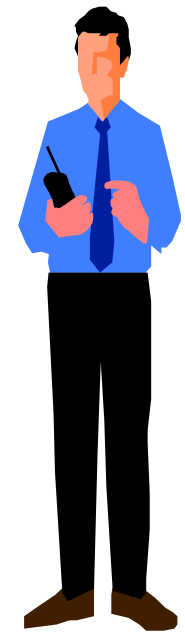
$A = g^{a} \bmod p$

$K = B^{a} \bmod p$

A → (Alice to Bob)

B ← (Bob to Alice)

BOB



b secret

$B = g^{b} \bmod p$

$K = A^{b} \bmod p$

Security of Diffie-Hellman Key Exchange

- If the Discrete Logarithm Problem (DLP) is easy then DH key exchange (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 DLP 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.

Man-in-the-Middle in the DH KE

Alice | Carl (man-in-the-middle) | Bob

Alice: a, g^a

Alice → Carl: g^a

Carl: c, g^c

Carl → Bob: g^{c1}

Bob: b, g^b

Bob → Carl: g^b

Carl: d, g^d

Carl → Alice: g^d

Alice: $K_2 = (g^d)^a$

Carl: $K_1 = (g^b)^c$

Carl: $K_2 = (g^a)^d$

Bob: $K_1 = (g^c)^b$

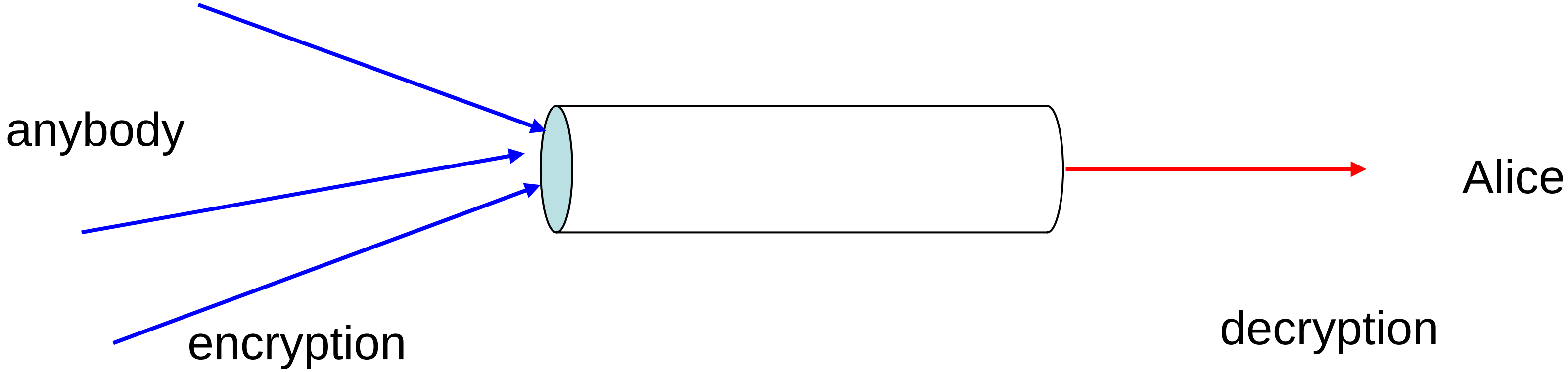
Alice ↔ Carl: Encryption using K_2

Carl ↔ Bob: Encryption using K_1

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.

Setting up the ElGamal public key cryptosystem

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

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

Standard "modulo p" groups and their generators can be found in: [RFC3526] RFC 3526: More Modular Exponential Diffie-Hellman groups for Internet Key Exchange

Selecting parameters for Discrete Log based cryptosystem

- p and g can be the same for many users, but need not be.
- If p -1 has many small factors, then the probability that a public key generates a small group is non-negligble. To avoid this, the prime p is generated to be a *secure prime,* or *Sophie Germain prime.* Then $p = 2q + 1$, where q is a prime.
- All primes p given in RFC 3526 are Sophie Germain primes and the generator elements have prime order $q = \frac{1}{2}(p - 1)$.