CS579: Foundations of Cryptography

Spring 2023

Key Agreement

Instructor: **Nikos Triandopoulos**

STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY®
1870

Number theory background

Multiplicative inverses

The residues modulo a positive integer n comprise set $Z_n = \{0,1,2,\ldots,n - 1\}$

- let x and y be two elements in Z_n such that $x\ y \bmod n = 1$
  - we say: y is the multiplicative inverse of x in Z_n
  - we write: $y = x^{-1}$
- example:
  - multiplicative inverses of the residues modulo 11

x	0	1	2	3	4	5	6	7	8	9	10
x^{-1}		1	6	4	3	9	2	8	7	5	10

Multiplicative inverses (cont'ed)

Theorem

An element x in Z_n has a multiplicative inverse iff x, n are relatively prime

- e.g.
  - the only elements of Z_{10} having a multiplicative inverse are 1, 3, 7, 9

x	0	1	2	3	4	5	6	7	8	9
x^{-1}		1		7				3		9

Corollary

If p is prime, every non-zero residue in Z_p has a multiplicative inverse

Theorem

A variation of Euclid's GCD algorithm computes the multiplicative inverse of an element x in Z_n or determines that it does not exist

Euclid's GCD algorithm

Computes the greater common divisor by repeatedly applying the formula

gcd(a, b) = gcd(b, a mod b)

- example
  - gcd(412, 260) = 4

```
Algorithm EuclidGCD(a, b)
    Input integers a and b
    Output gcd(a, b)

    if b = 0
        return a
    else
        return EuclidGCD(b, a mod b)
```

a	412	260	152	108	44	20	4
b	260	152	108	44	20	4	0

Extended Euclidean algorithm

Theorem

If, given positive integers **a** and **b**, **d** is the smallest positive integer s.t. **d** = **ia** + **jb**, for some integers **i** and **j**, then **d** = gcd(**a, b**)

- example
  - **a** = 21, **b** = 15
  - **d** = 3, **i** = 3, **j** = -4
  - 3 = 3·21 + (-4)·15 = 63 - 60 = 3

Algorithm **Extended-Euclid**(a, **b**)

- **Input** integers **a** and **b**
- **Output** gcd(**a**, **b**), i and j s.t. ia+jb = gcd(a,b)

```
if b = 0
    return (a,1,0)
(d′, x′, y′) =  Extended-Euclid(b, a mod b)
(d, x, y) = (d′, y′, x′ - [a/b]y′)
return (d, x, y)
```

Computing multiplicative inverses

Fact

- given two numbers **a** and **b**, there exist integers x, y s.t.

$$x\,a + y\,b = \gcd(a,b)$$

which can be computed efficiently by the extended Euclidean algorithm

Thus

- the multiplicative inverse of a in Z_b exists iff gcd(a, b) = 1
- i.e., iff the extended Euclidean algorithm computes x and y s.t. $x\,a + y\,b = 1$
- in this case, the multiplicative inverse of a in Z_b is x

Multiplicative group

A set of elements where multiplication • is defined

- closure, associativity, identity & inverses
- multiplicative groups Z^*_n, defined w.r.t. Z_n (residues modulo n)
  - subsets of Z_n containing all integers that are relative prime to n
  - if n is a prime number, then all non-zero elements in Z_n have an inverse
    - $Z^*_7 = \{1,2,3,4,5,6\}$, $n = 7$
    - $2 \bullet 4 = 1 \pmod 7$, $3 \bullet 5 = 1 \pmod 7$, $6 \bullet 6 = 1 \pmod 7$, $1 \bullet 1 = 1 \pmod 7$
  - if n is not prime, then not all integers in Z_n have an inverse
    - $Z^*_{10} = \{1,3,7,9\}$, $n = 10$
    - $3 \bullet 7 = 1 \pmod{10}$, $9 \bullet 9 = 1 \pmod{10}$, $1 \bullet 1 = 1 \pmod{10}$

Order of a multiplicative group

Order of a group: cardinality of group

- multiplicative groups for Z^*_n
- the totient function $\phi(n)$ denotes the order of Z^*_n , i.e., $\phi(n) = |Z^*_n|$
  - if $n = p$ is prime, then the order of $Z^*_p=\{1,2,\ldots,p-1\}$ is $p-1$, i.e., $\phi(n) = p-1$
    - e.g., $Z^*_7 = \{1,2,3,4,5,6\}$, $n = 7$, $\phi(7) = 6$
  - if n is not prime, $\phi(n) = n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$, where $n = p^{e1}{}_1p^{e2}{}_2\ldots p^{ek}{}_k$
    - e.g., $Z^*_{10} = \{1,3,7,9\}$, $n = 10$, $\phi(10) = 4$
- if $n = p\,q$, where p and q are distinct primes, then $\phi(n) = (p-1)(q-1)$
  - difficult problem: given $n = pq$, where p, q are primes, find p and q or $\phi(n)$

Fermat's Little Theorem

Theorem

If p is a prime, then for each nonzero x in Z_p, we have $x^{p-1} \bmod p = 1$

- example (p = 5):

$1^4 \bmod 5 = 1$ $\quad$ $2^4 \bmod 5 = 16 \bmod 5 = 1$

$3^4 \bmod 5 = 81 \bmod 5 = 1$ $\quad$ $4^4 \bmod 5 = 256 \bmod 5 = 1$

Corollary

If p is a prime, then the multiplicative inverse of each non-zero residue x in Z_p is $x^{p-2} \bmod p$

- proof: $x(x^{p-2} \bmod p) \bmod p = xx^{p-2} \bmod p = x^{p-1} \bmod p = 1$

Euler's Theorem

Theorem

For each element x in Z^*_n, we have $x^{\phi(n)} \bmod n = 1$

- example (n = 10)
  - $Z^*_{10} = \{1,3,7,9\}$, n = 10, $\phi(10) = 4$
  - $3^{\phi(10)} \bmod 10 = 3^4 \bmod 10 = 81 \bmod 10 = 1$
  - $7^{\phi(10)} \bmod 10 = 7^4 \bmod 10 = 2401 \bmod 10 = 1$
  - $9^{\phi(10)} \bmod 10 = 9^4 \bmod 10 = 6561 \bmod 10 = 1$

Computing in the exponent

For the multiplicative group Z^*_n, we can reduce the exponent modulo $\phi(n)$

- $x^y \bmod n = x^{k\,\phi(n) + r} \bmod n = (x^{\phi(n)})^k x^r \bmod n = x^{r \bmod \phi(n)} \bmod n$

Corollary: For Z^*_p, we can reduce the exponent modulo p-1

- example
  - $Z^*_{10} = \{1,3,7,9\}$, $n = 10$, $\phi(10) = 4$
  - $3^{1590} \bmod 10 = 3^{1590 \bmod 4} \bmod 10 = 3^2 \bmod 10 = 9$
  - how about 2^8 mod 10?
- example
  - $Z^*_p = \{1,2,\ldots,p - 1\}$, $p = 19$, $\phi(19) = 18$
  - $15^{39} \bmod 19 = 15^{39 \bmod 18} \bmod 19 = 15^3 \bmod 19 = 12$

Powers

Let p be a prime

- the sequences of successive powers of the elements in Z^*_p exhibit repeating subsequences
- the sizes of the repeating subsequences and the number of their repetitions are the divisors of p – 1
- example, p = 7

x	x^2	x^3	x^4	x^5	x^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

The Discrete Log problem & its applications

The discrete logarithm problem

Setting

- if p be an odd prime, then $G = (Z_p^*, \cdot)$ is a cyclic group of order $p - 1$
  - $Z_p^* = \{1, 2, 3, \ldots, p-1\}$, generated by some g in Z_p^*
    - for $i = 0, 1, 2, \ldots, p-2$, the process **$g^i \bmod p$** produces all elements in Z_p^*
  - for any x in the group , we have that **$g^k \bmod p = x$**, for some integer k
  - k is called the **discrete logarithm** (or log) of x (mod p)

Example

- $(Z_{17}^*, \cdot)$ is a cyclic group G with order 16, 3 is the generator of G and $3^{16} = 1 \bmod 17$
- let $k = 4$, $3^4 = 13 \bmod 17$ (which is easy to compute)
- the inverse problem: if $3^k = 13 \bmod 17$, what is k? what about **large p**?

Computational assumption

Discrete-log setting

- cyclic $G = (Z_p^*, \cdot)$ of order $p - 1$ generated by g, prime p of length t ($|p|=t$)

Problem

- given G, g, p and x in Z_p^*, compute the discrete log k of x (mod p)

Discrete log assumption

- for groups of specific structure, **solving the discrete log problem is infeasible**
- any efficient algorithm finds discrete logs negligibly often (prob = $2^{-t/2}$)

Brute force attack

- cleverly enumerate and **check $O(2^{t/2})$ solutions**

ElGamal encryption

Assumes discrete-log setting (cyclic $G = (Z_p^*, \cdot) = <g>$, prime p, message space Z_p)

Gen

- <u>secret key</u>: random number $x \in Z^*_p$ <u>public key</u>: $A = g^x \bmod p$, along w/ G, g, p

Enc

- pick a fresh <u>random</u> $r \in Z^*_p$ and set $R = A^r$ $(= g^{xr})$
- send ciphertext $\mathbf{Enc_{PK}(m) = (c_1, c_2)}$ where $\mathbf{c_1 = g^r}$, $\mathbf{c_2 = m \cdot R \bmod p}$

Dec

- $\mathbf{Dec_{SK}(c_1,c_2) = c_2\,(1/c_1^x) \bmod p}$ where $\mathbf{c_1^x = g^{xr}}$

Security is based on **Computational Diffie-Hellman** (CDH) assumption

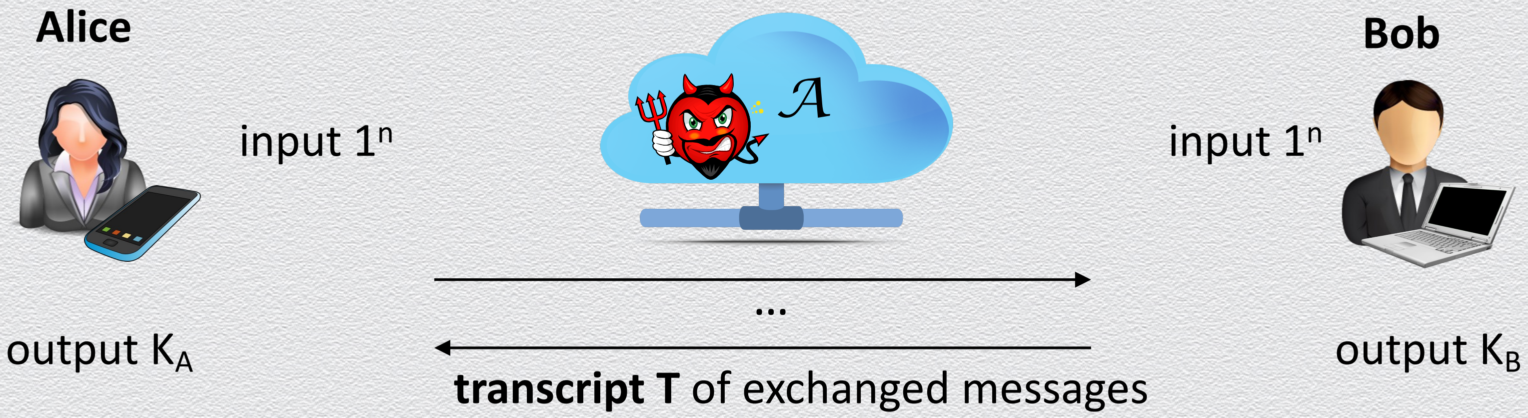
- given (g, g^a, g^b) it is hard to compute g^{ab}

A signature scheme can be also derived based on above discussion

Application: Key-agreement (KA) scheme

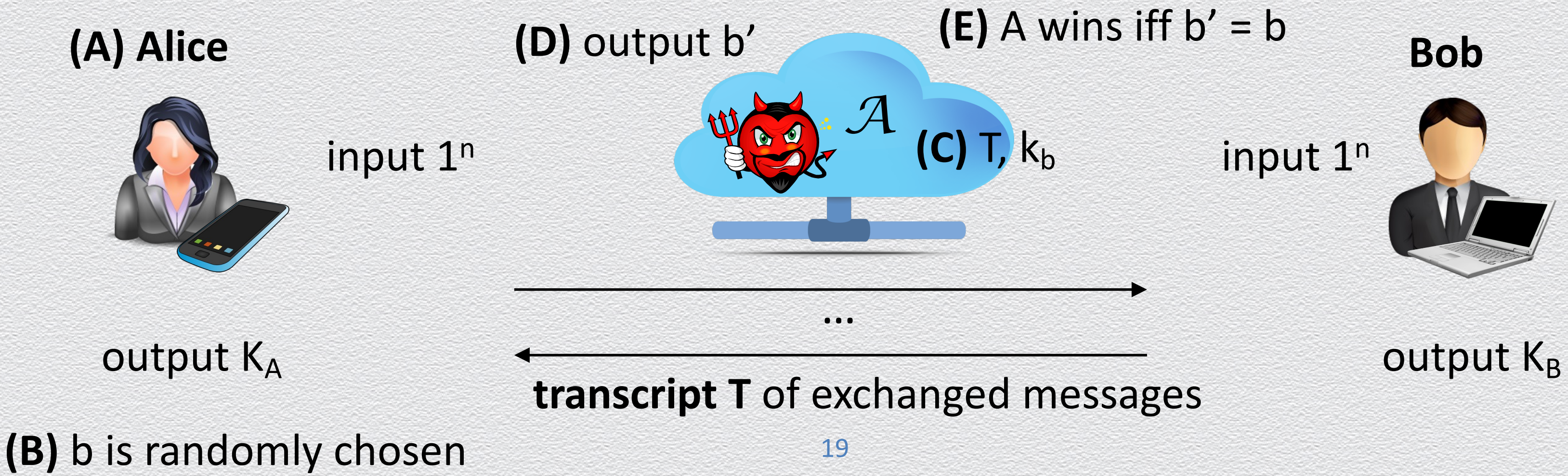
Alice and Bob want to securely establish a **shared key** for secure chatting over an **insecure** line

- instead of meeting in person in a secret place, they want to use the insecure line…
- KA scheme: they run a key-agreement protocol Π to contribute to a shared key K
- correctness: $K_A = K_B = K$
- security: no PPT adversary $\mathcal{A}$, given T, can distinguish K from a trully random one



Key agreement: Game-based security definition

- scheme $\Pi(1^n)$ runs to generate $K = K_A = K_B$ and transcript T; random bit b is chosen
- adversary $\mathcal{A}$ is given T and k_b; if b = 1, then $k_b = K$, else k_b is random (both n-bit long)
- $\mathcal{A}$ outputs bit b' and wins if b' = b
- then: **Π is secure if no PPT A has non-negligible advantage than guessing**



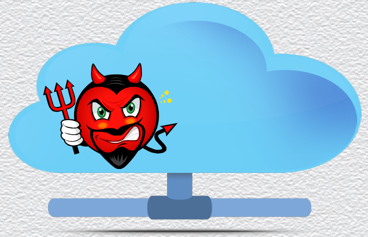
The Diffie-Hellman key-agreement protocol

Alice and Bob want to securely establish a **shared key** for secure chatting over an **insecure** line

- DH KA scheme Π
  - discrete log setting: p, g public, where <g> = Z^*_p and p prime

Alice

input 1^n



Bob

input 1^n

(1) randomly pick secret a

(2) randomly pick secret b

(3) send g^a mod p →

← **(4)** send g^b mod p

(5) set **K = g^{ab} mod p** = (g^b mod p)^a mod p

(6) set **K = g^{ab} mod p** = (g^a mod p)^b mod p

Security

- discrete log assumption is necessary but not sufficient
- decisional DH assumption
  - given g, g^a and g^b, g^{ab} is computationally indistinguishable from uniform

Authenticated Diffie-Hellman