Diffie-Hellman Key Exchange

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@.unipi.it

Version: 2024-04-04

1

Preliminaries

- Whitfield Diffie and Martin Hellman, New directions in cryptography, IEEE Transactions of Information Theory, 22(6), pp. 644-654, Nov. 1976
- Cryptosystem for key establishment
- One-way function
  - f: discrete exponentiation is computationally "easy"
  - f^{-1}: discrete logarithm it is computationally "difficult"

2

Preliminaries

- Mathematical foundation
  - Abstract algebra: groups, sub-groups, finite groups and cyclic groups
- We operate in the *multiplicative group* $\mathbb{Z}_p^*$ with addition and multiplication modulo p, with p prime
  - $\mathbb{Z}_p^*$ is the set of integers i belonging to [0, …, p – 1], s.t. gcd(i, p) = 1
  - Ex. Z^*_{11} = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

April 24 Diffie-Hellman Key Exchange 3

3

Facts on modular arithmetic

- Multiplication is commutative
  - $(a \times b) \equiv (b \times a) \bmod n$
- Exponentiation is commutative
  - $(a^x)^y \equiv (a^y)^x \bmod n$
- Power of power is commutative
  - $(a^b)^c \equiv a^{bc} \equiv a^{cb} \equiv (a^c)^b \bmod n$

April 24 Diffie-Hellman Key Exchange 4

4

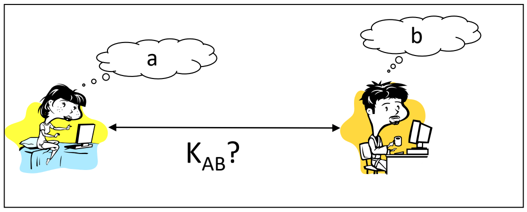
Facts on modular arithmetic

- Parameters
  - Let p be prime and $g \in \mathbb{Z}_p^*$ be a *primitive element* (or *generator*), i.e., for each $y \in \mathbb{Z}_p^*$ there is $x \in \mathbb{Z}_p^*$ s.t. $y \equiv g^x \bmod p$
- Discrete Exponentiation
  - Given $x \in \mathbb{Z}_p^*$, compute $y \in \mathbb{Z}_p^*$ s.t. $y = g^x \bmod p$
- Discrete Logarithm Problem (DLP)
  - Given $y \in \mathbb{Z}_p^*$, determine $x \in \mathbb{Z}_p^*$ s.t. $y = g^x \bmod p$
    - Notation $x = \log_g y \bmod p$

Properties of discrete log

- $\log_g(\beta\gamma) \equiv (\log_g\beta + \log_g \gamma) \bmod p$
- $\log_g(\beta)^s \equiv s\,(\log_g\beta) \bmod p$

The Diffie-Hellman Protocol



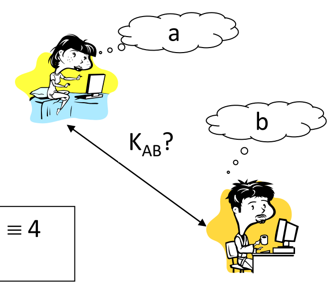
SETUP

- Let p be a large prime (600 digits, 2000 bits)
- Let 1 < g < p a generator
- Let p and g be publicly known

- THE DIFFIE-HELLMAN KEY EXCHANGE (DHKE)
  - Alice chooses a random secret number a (private key)
  - Bob chooses a random secret number b (public key)
  - M1: Alice $\rightarrow$ Bob: A, $Y_A \equiv g^a \bmod p$ (public key)
  - M2: Bob $\rightarrow$ Alice: B, $Y_B \equiv g^b \bmod p$ (public key)
  - Alice computes $K_{AB} \equiv (Y_B)^a \equiv g^{ab} \bmod p$
  - Bob computes $K_{AB} \equiv (Y_A)^b \equiv g^{ab} \bmod p$

7

DHKE with small numbers



Let p = 11, g = 7

Alice chooses a = 3 and computes $Y_A \equiv g^a \equiv 7^3 \equiv 343 \equiv 2 \bmod 11$

Bob chooses b = 6 and computes $Y_B \equiv g^b \equiv 7^6 \equiv 117649 \equiv 4 \bmod 11$

A $\rightarrow$B: 2
B $\rightarrow$A: 4

Alice receives 4 and computes $K_{AB} = (Y_B)^a \equiv 4^3 \equiv 9 \bmod 11$

Bob receives 2 and computes $K_{AB} = (Y_A)^b \equiv 2^6 \equiv 9 \bmod 11$

8

DHKE computational aspects

- Large prime *p* can be computed as for RSA
- Exponentiation can be computed by square-and-multiply
  - The trick of using small exponents is non applicable here
- $\mathbb{Z}_p^*$ is cyclic
  - g is a generator, g^i mod p defines a permutation
    - p = 11, g = 2
      - $2^1 \equiv 2 \bmod 11$ $2^5 \equiv 10 \bmod 11$ $2^9 \equiv 6 \bmod 11$
      - $2^2 \equiv 4 \bmod 11$ $2^6 \equiv 9 \bmod 11$ $2^{10} \equiv 1 \bmod 11$
      - $2^3 \equiv 8 \bmod 11$ $2^7 \equiv 7 \bmod 11$ *repeat cyclically*
      - $2^4 \equiv 5 \bmod 11$ $2^8 \equiv 3 \bmod 11$

Security of DHKE

- Intuition
  - Eavesdropper sees p, g, Y_A and Y_B and wants to compute K_{AB}
- Diffie-Hellman Problem (DHP)
  - Given p, g, $Y_A \equiv g^a \bmod p$ and $Y_B \equiv g^b \bmod p$, compute $K_{AB} = g^{ab} \bmod p$
- How hard is this problem?

Security of DHKE

- DHP $\leq_P$ DLP
  - If DLP can be easily solved, then DHP can be easily solved
  - There is no proof of the converse, i.e., if DLP is difficult then DHP is difficult
  - At the moment, we don't see any way to compute K_{AB} from Y_A and Y_B without first obtaining either a or b

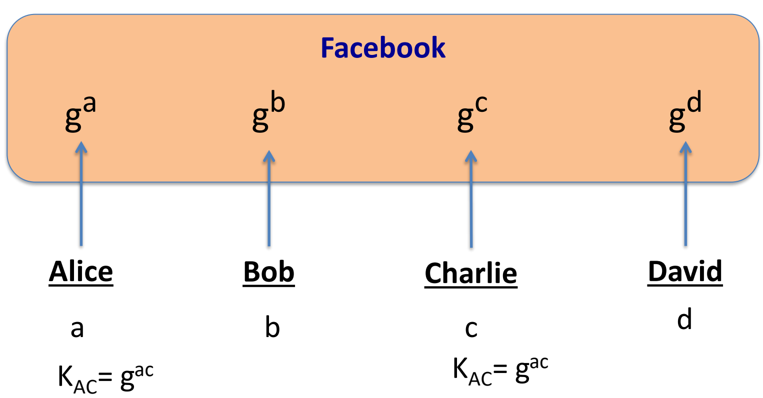
DLP – rule of thumb

- Let p be a prime on t bits ($p < 2^t$)
- Exponentiation takes at most $2 \cdot \log_2 p < 2t$ long integer multiplications (mod p)
  - Linear in the exponent size (t)
- Discrete logs require $\sqrt{p} = 2^{t/2}$ multiplication
- Example n = 512
  - Exponentiation: #multiplications ≤ 1024
  - Discrete log: #multiplications $\approx 2^{256} = 10^{77}$
    - 10^{17} seconds since Big Bang

Diffie-Hellman Key Exchange

NOT-INTERACTIVITY

Diffie-Hellman is not-interactive

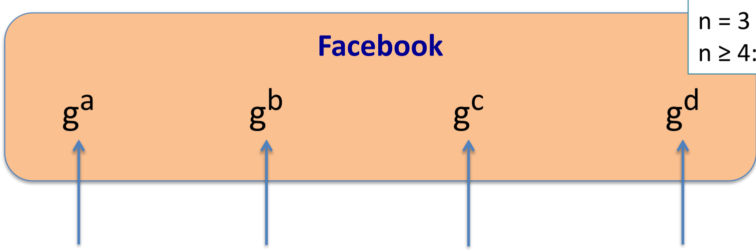


Not-interactive protocol: in order to obtain a shared key with Bob, Alice does not need to receive any message from Bob

Diffie-Hellman is not interactive

Non-interactive group DH for groups larger than 3 members is still an open problem

n = 2 (DH)
n = 3 (Joux)
$n \geq 4$: open



Alice	Bob	Charlie	David
a	b	c	d
K_{ABCD}	K_{ABCD}	K_{ABCD}	K_{ABCD}

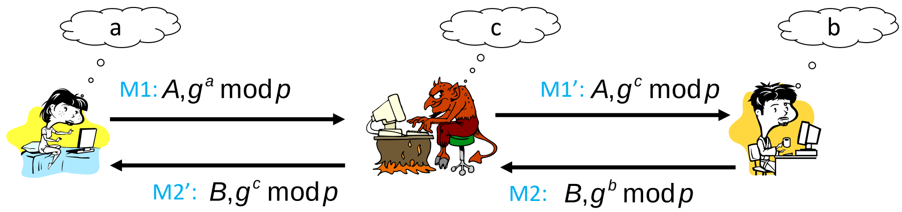
15

Diffie-Hellman Key Exchange

THE MAN-IN-THE-MIDDLE ATTACK

16

Man-in-the-Middle Attack

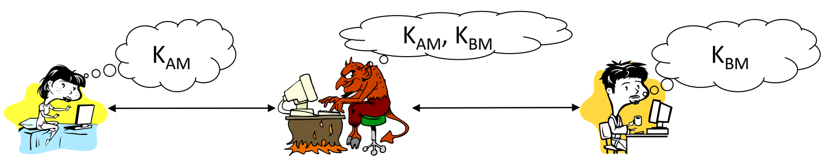


$K_{AM} = g^{ac} \bmod p$

$K_{AM} = g^{ac} \bmod p$, e
$K_{BM} = g^{bc} \bmod p$

$K_{BM} = g^{bc} \bmod p$

Man-in-the-Middle Attack



- Beliefs
  - Alice believes to communicate with Bob by means of K_{AM}
  - Bob believes to communicate with Alice by means of K_{BM}
- The adversary can
  - read messages between Alice and Bob
  - impersonate Alice or Bob
- DHKE is insecure against MIM (active) attack

Man-in-the-Middle Attack

- The attack is possible because
  - Y_A and Y_B are not authenticated
  - A and Y_A, as well as B and Y_B, are not indissolubly linked
    - A: Alice's identifier
    - B: Bob's identifier
  - Two sides of the same coin

April 24 Diffie-Hellman Key Exchange 19

19

MitM: possible solutions [→]

- PROTOCOL USING DIGITAL SIGNATURES
- The protocol
  - Alice → Bob: $Y_A, \langle Y_A, B \rangle_A$
  - Bob → Alice: $Y_B, \langle Y_A, Y_B, A \rangle_B$
  - With $\langle X \rangle_P$ digital signature on statement X by principal P
- Critical issue
  - Authenticiy of public keys

April 24 Diffie-Hellman Key Exchange 20

20

MitM: possible solutions [→]

- PROTOCOL USING PASSWORDS
- Let w be a secret shared password between Alice and Bob
- The protocol
  - Alice → Bob: $Enc_w(Y_A)$
  - Bob → Alice: $Enc_w(Y_B)$

MitM: possible solutions

- PROTOCOL USING PASSWORDS
- Properties
  - The protocol is robust against password guessing attack
    - As Y is random (and unknown to the adversary), this value does give no information to the adversary
    - An adversary cannot perfom an off-line password attack

Diffie-Hellman Key Exchange

THE GENERALIZED DLP AND RELATED ATTACKS

The Generalized DLP

- DLP can be defined on any cyclic group
- GDLP (def)
  - Given a finite cyclic group G with group operation • and cardinality n, i.e., |G| = n.
  - We consider a *primitive element* $\alpha \in G$ and another element $\beta \in G$. The discrete logarithm problem is finding the integer x, where $1 \leq x \leq n$, such that

$$\beta = \underbrace{\alpha \bullet \alpha \bullet \alpha \bullet \ldots \bullet \alpha}_{\text{x times}} = \alpha^x$$

DLP for cryptography

- Multiplicative prime group $\mathbb{Z}_p^*$
  - DHKE, ElGamal encryption, Digital Signature Algorithm (DSA)
- Cyclic group formed by Elliptic curves
- Galois field GF(2^m)
  - Equivalent to $\mathbb{Z}_p^*$
  - Attacks against DLP in GF(2^m) are more powerful than DLP in $\mathbb{Z}_p^*$ so we need "higher" bit lengths than $\mathbb{Z}_p^*$
- Hyperelliptic curves or algebraic varieties

April 24 Diffie-Hellman Key Exchange 25

25

Algorithms for DLP

- Generic Algorithms work in any cyclic group:
  - Brute-force Search
  - Shank's Baby-Step Giant-Step Method
  - Pollard's Rho Method
  - Pohlig-Hellman Algorithm
- Nongeneric algorithms exploit inherent structure of certain groups
- FACT – Difficulty of DLP is independent of the generator

April 24 Diffie-Hellman Key Exchange 26

26

Algorithms for DLP

- GENERIC ALGORITHMS
- Brute-force Search
  - Running time: $O(|G|)$
- Shank's Baby-Step Giant-Step Method
  - Running time: $O\left(\sqrt{|G|}\right)$
  - Storage: $O\left(\sqrt{|G|}\right)$

%

April 24 Diffie-Hellman Key Exchange 27

27

Algorithms for DLP

- GENERIC ALGORITHMS
- Pollard's Rho Method
  - Based on the Birthday Paradox
  - Running time: $O\left(\sqrt{|G|}\right)$
  - Storage: negligible

April 24 Diffie-Hellman Key Exchange 28

28

Algorithms for DLP

- GENERIC ALGORITHMS
- Pohlig-Hellman Algorithm
  - Based on CRT, exploits factorization of |G| = $\prod_{i=1}^{r}(p_i)^{e_i}$
    - Reduces DLP to DLP in (smaller) groups of order ${p_i}^{e_i}$
    - In the EC, computing |G| is not easy
  - Running time: $\mathcal{O}\left(\sum_{i=1}^{r} e_i \cdot \left(lg|G| + \sqrt{p_i}\right)\right)$
    - Efficient if each p_i is «small» ➔
    - The *smallest factor* of |G| must be in the range 2^{160}

April 24 Diffie-Hellman Key Exchange 29

29

Algorithms for DLP

- NONGENERIC ALGORITHMS
  - Exploit inherent structure of certain groups
- The Index-Calculus Method
  - Very efficient algorithm to compute DLP in $\mathbb{Z}_p^*$ and GF(2^m)
  - Sub-exponential running time
    - In $\mathbb{Z}_p^*$, to achieve 80-bit security, the prime p must be at least 1024 bit long
    - It is even more efficient in GF(2^m) ➔ For this reason, DLP in GF(2^m) are not used in practice

April 24 Diffie-Hellman Key Exchange 30

30

Diffie-Hellman Key Exchange

DLP IN SUBGROUPS

Cyclic groups

- Theorem 8.2.2. For every prime p, $(\mathbb{Z}_p^*, \times)$ is an abelian finite cyclic group
  - **Finite**: contains a finite number of elements
  - **Group**: closed, associative, identity element, inverse, commutative (abelian)
  - **Cyclic**: contain an element α with *maximum order* ord(α) = $|\mathbb{Z}_p^*|$ = $p - 1$, where *order of a* $\in \mathbb{Z}_p^*$, ord(a) = k, is the smallest positive integer k such that $a^k \equiv 1 \bmod p$
    - α is called *generator* or *primitive element*
  - The notion of finite cyclic group is generalizable to (G, •)

Cyclic groups – order

- Example: consider $\mathbb{Z}_{11}^{*}$ and a = 3
  - $a^1 = 3$
  - $a^2 = a \cdot a = 3 \cdot 3 = 9$
  - $a^3 = a^2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \bmod 11$
  - $a^4 = a^3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \bmod 11$
  - $a^5 = a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \bmod 11$ ← ord(3) = 5
  - $a^6 = a^5 \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11$
  - $a^7 = a^5 \cdot a^2 \equiv 1 \cdot a^2 \equiv 9 \bmod 11$
  - $a^8 = a^5 \cdot a^3 \equiv 1 \cdot a^3 \equiv 5 \bmod 11$
  - $a^9 = a^5 \cdot a^4 \equiv 1 \cdot a^4 \equiv 4 \bmod 11$
  - $a^{10} = a^5 \cdot a^5 \equiv 1 \cdot 1 \equiv 1 \bmod 11$ ← periodic
  - $a^{11} = a^{10} \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11$
  - 3^i generates the periodic sequence {3, 9, 5, 4, 1}

Length of the sequence = 5

33

Cyclic groups – primitive element

- Example
- Consider $\mathbb{Z}_{11}^{*}$ and a = 2
  - $a = 2$
  - $a^2 = 4$
  - $a^3 = 8$
  - $a^4 \equiv 5 \bmod 11$
  - $a^5 \equiv 10 \bmod 11$

  $a^6 \equiv 9 \bmod 11$
  $a^7 \equiv 7 \bmod 11$
  $a^8 \equiv 3 \bmod 11$
  $a^9 \equiv 6 \bmod 11$
  $a^{10} \equiv 1 \bmod 11$ ← ord(2) = 10
- ord(2) = 10 = | $\mathbb{Z}_{11}^{*}$ | → a = 2 is a primitive element
- The sequence contains all elements of $\mathbb{Z}_{11}^{*}$

34

Cyclic groups – permutation

Powers of a primitive element define a *permutation* of the elements of $\mathbb{Z}_p^*$

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

April 24 Diffie-Hellman Key Exchange 35

35

Cyclic groups – order and generators

- Order of elements of $\mathbb{Z}_{11}^*$
  - ord(1) = 1 ord(6) =10
  - ord(2) = 10 ord(7) =10
  - ord(3) = 5 ord(8) =10
  - ord(4) = 5 ord(9) = 5
  - ord(5) = 5 ord(10) = 2
- Any order is a divisor of $|Z_{11}{}^*|$ = 10 → {1, 2, 5, 10}
- #(primitive elements) is Φ(10) = $\Phi(|\mathbb{Z}_{11}^*|)$ = 4
- Set of primitive elements = {2, 6, 7, 8}

April 24 Diffie-Hellman Key Exchange 36

36

Cyclic groups

- Theorem 8.2.3
  - Let G be a finite group. Then for every $a \in G$ it holds that:
  - 1. $a^{|G|} = 1$ (Generalization of Fermat's Little Theorem)
  - 2. ord(a) divides $|G|$
- Theorem 8.2.4
  - Let G be a finite cyclic group. Then it holds that
    1. The number of primitive elements of G is $\Phi(|G|)$.
    2. If $|G|$ is prime, then all elements $a \neq 1 \in G$ are primitive.

Subgroups

- Theorem 8.2.5 Cyclic Subgroup Theorem
  - Let G be a cyclic group. Then every element a ∈ G with ord(a) = s is the primitive element of a cyclic subgroup with s elements.
  - Example
    - $\mathbb{Z}_{11}^*$, a = 3, s = ord(3) = 5, H = {1,3,4,5,9}
    - H is a finite, cyclic subgroup of order 5

Subgroups

- Theorem 8.2.6 (Lagrange's theorem)
  - Let H be a subgroup of G. Then $|H|$ divides $|G|$.
- Example: $\mathbb{Z}_{11}^{*}$
  - $|\mathbb{Z}_{11}^{*}| = 10$ whose divisors are 1, 2, 5 (and 10)

Subgroup	elements	primitive element
H_1	{1}	$\alpha = 1$
H_2	{1, 10}	$\alpha = 10$
H_5	{1, 3, 4, 5, 9}	$\alpha = 3, 4, 5, 9$

April 24 Diffie-Hellman Key Exchange 39

39

Subgroups

- Theorem 8.2.7
  - Let G be a finite cyclic group of order n and let α be a generator of G. Then for every integer k that divides n there exists exactly one cyclic subgroup H of G of order k. This subgroup is generated by $\alpha^{n/k}$. H consists exactly of the elements $a \in G$ which satisfy the condition $a^k = 1$. There are no other subgroups.
- Example.
  - Given $\mathbb{Z}_{11}^{*}$, generator $\alpha = 8$ and k = 2, then $\beta = 8^{10/2} = 10 \bmod 11$ is a generator for H of order k = 2

April 24 Diffie-Hellman Key Exchange 40

40

Relevance of subgroups to DLP [→]

- Pohlig-Hellman Algorithm
  - Exploit factorization of $|G| = p_1^{e1} \cdot p_2^{e2} \cdot \ldots \cdot p_\ell^{e\ell}$
  - Run time depends on the size of prime factors
    - The smallest prime factor must be in the range 2^{160}
  - Then $|\mathbb{Z}_p^*| = p - 1$ is even ➔ 2 (small) is one of the divisors! ➔ It is advisable to work in a large prime subgroup H
    - If |H| is prime, $\forall a \in H$, a is a generator (Theorem 8.2.4)

Relevance of subgroups to DLP [→]

- SAFE PRIMES
- Definition: given a prime $p = 2 \cdot q+1$, where q is a prime then p is a *safe prime* and q is a *Sophie Germain prime*
- It follows that $\mathbb{Z}_p^*$ has a subgroup H_q of (large) prime order q

Relevance of subgroups to DLP [↓]

- SMALL SUBGROUP CONFINEMENT ATTACK
  - A (small) subgroup confinement attack on a cryptographic method that operates in a large finite group is where an attacker attempts to compromise the method by forcing a key to be confined to an unexpectedly small subgroup of the desired group.

April 24 Diffie-Hellman Key Exchange 43

43

Small Subgroup Confinement Attack against DHKE

- Consider prime p, $\mathbb{Z}_p^*$, and generator α

Alice **MIM** **Bob**

a ← random() b ← random()

$A \equiv \alpha^a$ mod p $B \equiv \alpha^b$ mod p

------A------------A'-------- >

K = $(A')^b$ mod p

<-------B'------------------B-----

K = $(B')^a$ mod p

< ------------------ E_K(*session*)---------------------- >

April 24 Diffie-Hellman Key Exchange 44

44

Small Subgroup Confinement Attack against DHKE

- Recall THEOREM 8.2.7
- The attack
  - Consider k that divides n = $|\mathbb{Z}_p^*|$ = p – 1 ➔
  - A' $\equiv A^{n/k} \equiv (\alpha^a)^{n/k} \equiv (\alpha^{n/k})^a$ mod p
  - B' $\equiv B^{n/k} \equiv (\alpha^b)^{n/k} \equiv (\alpha^{n/k})^b$ mod p
  - Session key K = β^{ab} mod p, with $\beta = \alpha^{n/k}$
  - $\beta = \alpha^{n/k}$ is a generator of subgroup H of order k ➔
  - DHKE gets confined in H_k and brute force becomes easier
  - It is advisable to work in a large prime subgroup H

A practical variant

- In the DHKEP, the key is defined as $K = H\left(g^{a \cdot b}\right)$ where H is a cryptographic hash function.
  - A practical choice is SHA-256
- Motivation: g^{ab} may not have enough entropy
  - If DHKEP is run in a subgroup Γ of $\mathbb{Z}_p^*$, then elements of Γ are represented on $\lceil \log_2(p+1) \rceil$ bits while $\mathrm{ord}(\Gamma) \ll p$.
  - The use of H is a practical way to remove such a redundancy provided that $\mathrm{ord}(\Gamma) \gg 2^k$