Cryptography Part VI: Diffie-Hellman

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75 # theory
- Handbook of Applied Cryptography, Chapter 12.6, pp. 515-523 Diffie Hellman
- (recommended) Introduction to Modern Cryptography, Chapters 8 and 10

thry

Diffie Hellman

Notation for Public Key Cryptography

- C_i is ciphertext message *i*
- P_i is plaintext message *i*
- E_{pk} is encryption with public key *pk*
  - Note that *E* is asymmetric
  - $E_{pk}(P_i) = C_i$

E_{pk}

- D_{sk} is decryption with secret key *sk*
  - Note that *D* is asymmetric
    - $D_{sk}(C_i) = P_i$

D_{sk}

- $\{X\}$ is a set of elements of type *X*
- | is "such that"; e.g., integer $i \mid 3 < i < 5$ implies that $i = 4$

Diffie-Hellman Key Agreement

- Also called exponential key exchange
- Ralph Merkle invented the concept in the 1970s and named it after Whitfield Diffie and Martin Hellman
- One of the first public key cryptosystems
  - RSA
  - GHCQ claims
- Provides a shared key
- Does not provide entity authentication

Basic Diffie-Hellman Key Agreement Protocol

- Handbook of Applied Cryptography, pg. 516, 12.47
- Summary: Bob and Alice send each other one message over an untrusted channel
- Result: shared secret K known to Bob and Alice but no one else
- First step
  - An appropriate large prime number p and generator α of $\mathbb{Z}_p^*$ (where $2 \leq \alpha \leq p\text{-}2$) are chosen and published

Some Mathematics Background

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
  - $\mathbb{Z}$ is the set of integers and is an infinite set
- $\mathbb{Z}_n$ are the integers modulo *n*
  - $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$
  - Mathematical operations (e.g., addition, subtraction and multiplication) in $\mathbb{Z}_n$ are performed modulo *n*
- Definition of the Euler phi function *Φ(n)* (also known as the Euler totient function)
  - For $n \geq 1$, *Φ(n)* = the number of integers in $[1, n]$ which are relatively prime to *n*
  - Two numbers *a* and *b* are said to be *relatively prime* or *coprime* if their greatest common divisor is one (if *gcd*(*a*,*b*) = 1)
- Facts
  - If *p* is prime, then *Φ(p)* = *p*-1
  - The Euler phi function is multiplicative, i.e., if *gcd*(*m*,*n*) = 1, then *Φ(mn)* = *Φ(m)Φ(n)*

$\mathbb{Z}$

$n = 2^{128}$

$gcd(25, 31) = 1$

Some Mathematics Background (cont'd 1)

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75
- Definition $\mathbb{Z}_n$
  - The *multiplicative group* of $\mathbb{Z}_n$ is $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$
  - In particular, if *n* is prime, then $\mathbb{Z}_n^* = \{a \mid 1 \le a \le n - 1\}$
- Definition $n = 13$
  - The *order* of $\mathbb{Z}_n^*$ is the number of elements in $\mathbb{Z}_n^*$, i.e., $|\mathbb{Z}_n^*|$
  - From the definition of the Euler phi function it follows that $|\mathbb{Z}_n^*| = \Phi(n)$
  - Note that if $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n^*$ then $a \cdot b \in \mathbb{Z}_n^*$, i.e., $\mathbb{Z}_n^*$ is closed under multiplication (recall that all multiplication in $\mathbb{Z}_n$ is mod n)
- Example 1: $\mathbb{Z}_{21}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$
- Example 2: $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

$a \in \mathbb{Z}_n^*$

$b \in \mathbb{Z}_n^*$

$\Rightarrow a * b \bmod n \in \mathbb{Z}_n^*$

$19 \in \mathbb{Z}_{21}^*$

$20 \in \mathbb{Z}_{21}^*$

for every a there exists b s.t. $ab = 1$

$19 \cdot 20 = 380$ $\quad 19 \cdot 20 \bmod 21 = 2$ $\quad b = a^{-1}$

$21 \times 18 = 378$

Some Mathematics Background (cont'd 2)

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75
- Definition
  - If α is a generator of $\mathbb{Z}_n^*$, then $\mathbb{Z}_n^* = \{\alpha^i \; mod \; n \mid 0 \le i \le \emptyset(n) - 1\}$

6 is a generator of $Z_{13}^* \Rightarrow \{6^i \bmod 13,\; 0 \le i \le 11\}$

13 is prime $\Rightarrow \emptyset(n) = n-1 = 12$

- Example
  - α = 6 is generator of $\mathbb{Z}_{13}^*$

i		0	1	2	3	4	5	6	7	8	9	10	11
$\alpha^i \; mod \; 13$		1	6	10	8	9	2	12	7	3	5	4	11

  - Recall that $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

$6^0 =$ $\quad 6^1 \quad 6^2 \bmod 13$

6^i w/out knowing i, could be any element of Z_{13}^*

$6^{12} \bmod 13 = (6^2)^6 \bmod 13$

$(6^2 \bmod 13)^6 \bmod 13$

$\rightarrow (36 \bmod 13)^6 \bmod 13$

$(10)^6 \bmod 13 =$

Now Back to Diffie-Hellman Key Exchange…

$p=13$ $\alpha=6$ $\mathbb{Z}^*_{13}$

- First step
  - An appropriate prime number p and generator α of $\mathbb{Z}_p^*$ (where $2 \le \alpha \le p$-2) are chosen and published

Alice
x
alicenum $=\alpha^x \bmod p$

Public
p
α

- Protocol messages
  - Alice sends message to Bob: $\alpha^x \bmod p$ (Step **1**)
  - Bob send message to Alice: $\alpha^y \bmod p$ (Step **2**)

bob
y
bobnum $=\alpha^y \bmod p$

- Protocol actions each time a shared key is required
  - Alice chooses a random secret x, $1 \le x \le p$-2, and carries out Step **1**
  - Bob chooses a random secret y, $1 \le y \le p$-2, and carries out Step **2**
  - Bob receives $\alpha^x \bmod p$ and computes the shared secret $K = (\underbrace{\alpha^x \bmod p}_{\text{alicenum}})^y \bmod p = (\alpha^x)^y \bmod p$
  - Alice receives $\alpha^y \bmod p$ and computes the shared secret $K = (\underbrace{\alpha^y \bmod p}_{\text{bobnum}})^x \bmod p = (\alpha^y)^x \bmod p$

Alice

x

α, p

alicenum

Bob

y

bobnum

adversary

?

Discrete Logarithm Problem

given a, α, p

where $a = (\alpha^{Y} \bmod p)$

Question: $Y = ?$

4096 bits

$Y = \log_{\alpha}(\alpha^{Y})$

$a \in \mathbb{Z}_p^*$

$|\{4096 \text{ bits}\}|$

$O(2^{4096})$

RSA prime p prime q

$n = pq$

$n \quad \{2^{4094}, 1\}$

$p \geq 2^{4094} \qquad q \geq 2^{4094}$

Diffie-Hellman Key Exchange Preserves Forward Secrecy

CA

priv

K_i Jan 1 $\quad X_i \quad Y_i$

- If the adversary obtains shared secret K_i
  - e.g., through a lucky guess or through an insider (or any other means!)
- Result: shared secret K_j in the future is not also given away
- This is not true of other schemes
  - e.g., in an RSA public-private key scheme
  - giving away the private key does compromise future communications

Jun 5 $\quad X_j \quad Y_j$

K_j