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

©Georgia Institute of Technology, 2018-2024

Reading

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75
- Handbook of Applied Cryptography, Chapter 12.6, pp. 515-523
- Introduction to Modern Cryptography, Chapters 8 and 10

©Georgia Institute of Technology, 2018-2024

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
  - $E_{pk}(P_i) = C_i$
- D_{sk} is decryption with secret key sk
  - Note that D is asymmetric
    - $D_{sk}(C_i) = P_i$
- $\{X\}$ is a set of elements of type X
- | is “such that”; e.g., integer $i \mid 3 < i < 5$ implies that $i = 4$

©Georgia Institute of Technology, 2018-2024

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 authentication

©Georgia Institute of Technology, 2018-2024

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

©Georgia Institute of Technology, 2018-2024

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 $\Phi(n)$ (also known as the Euler totient function)
  - For $n \geq 1$, $\Phi(n)$ = 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 $\Phi(p) = p-1$
  - The Euler phi function is multiplicative, i.e., if $gcd(m,n) = 1$, then $\Phi(mn) = \Phi(m)\Phi(n)$

©Georgia Institute of Technology, 2018-2024
©Georgia Insitute of Technology, 2018

Some Mathematics Background (cont'd 1)

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75
- Definition
  - 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 $\mathbb{Z}_n^* = \{a \mid 1 \leq a \leq n - 1\}$
- Definition
  - 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: $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

©Georgia Institute of Technology, 2018-2024

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 $\mathbb{Z}_n^* = \{\alpha^i \, mod \, n \mid 0 \le i \le \emptyset(n) - 1\}$
- 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 $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

©Georgia Institute of Technology, 2018-2024

Now Back to Diffie-Hellman Key Exchange…

- First step
    - An appropriate prime number p and generator α of $\mathbb{Z}_p^*$ (where $2 \leq \alpha \leq p-2$) are chosen and published
- Protocol messages
    - Alice sends message to Bob: $\alpha^x \bmod p$ (Step **1**)
    - Bob send message to Alice: $\alpha^y \bmod p$ (Step **2**)
- Protocol actions each time a shared key is required
    - Alice chooses a random secret x, $1 \leq x \leq p-2$, and carries out Step **1**
    - Bob chooses a random secret y, $1 \leq y \leq p-2$, and carries out Step **2**
    - Bob receives $\alpha^x \bmod p$ and computes the shared secret $K = (\alpha^x \bmod p)^y \bmod p = (\alpha^x)^y \bmod p$
    - Alice receives $\alpha^y \bmod p$ and computes the shared secret $K = (\alpha^y \bmod p)^x \bmod p = (\alpha^y)^x \bmod p$

©Georgia Institute of Technology, 2018-2024

Diffie-Hellman Key Exchange Preserves Forward Secrecy

- 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

©Georgia Institute of Technology, 2018-2024