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
- Handbook of Applied Cryptography, Chapter 12.6, pp. 515-523 Difficence of the second sec

DVY

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* | 3 < *i* < 5 implies that *i* = 4



Diffie-Hellman Key Agreement

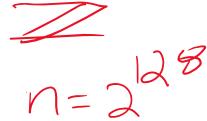
- Also called exponential key exchange
- <u>Ralph Merkle</u> invented the concept in the 1970s and named it after Whitfield Diffie and Martin Hellman
- One of the first public key cryptosystems
 - RSA
 - GHCQ claims
- Provides a shared key
- Does not provide authentication

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 $2 \le \alpha \le p-2$) 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 $\Phi(n)$ (also known as the Euler totient function)
 - For $n \ge 1$, $\Phi(n)$ = 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 qcd(a,b) = 1) (25) 31)=/
- Facts
- \rightarrow If p is prime then $\Phi(p) = p-1$
 - The Euler phi function is multiplicative, i.e., if gcd(m,n) = 1, then $\Phi(mn) = \Phi(m)\Phi(n)$



Some Mathematics Background (cont'd 1)

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75 a ezn
- Definition
 - The multiplicative group of \mathbb{Z}_n is $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

-> ax6 moly

a there

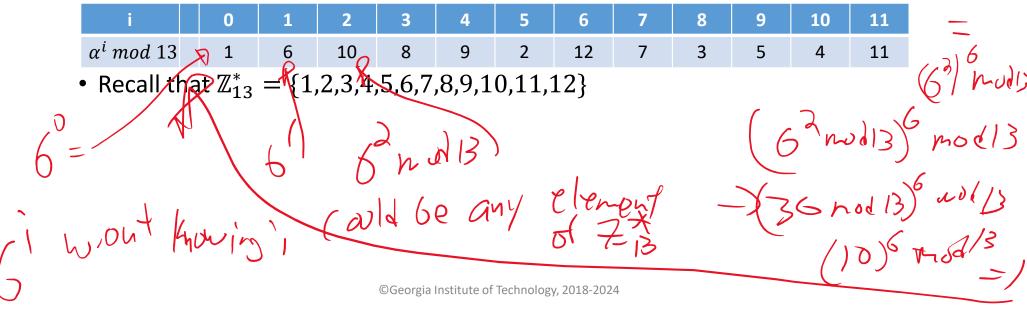
- In particular, if *n* is prime, then $\mathbb{Z}_n^* = \{a \mid 1 \le a \le n-1\}$ n = 13
- Definition
 - The *order* of \mathbb{Z}_n^* is the number of elements in \mathbb{Z}_n^* , i.e., \mathbb{Z}_n^*
 - From the definition of the Euler phi function it follows that $|\mathbb{Z}_n^*| = \mathcal{O}(n)$
- 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) for every
- Example 1: $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
- Example 2: $\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ [9.20=300 [9.20mod2]=2 6=a-1 exists 6 5.t. 96=1

Some Mathematics Background (cont'd 2)

- Handbook of Applied Cryptography, Chapter 2.4, pp. 63-75
 Definition 6 is a senerator of ZBA = 16
- - If α is a generator of \mathbb{Z}_n^* , then $\mathbb{Z}_n^* = \{ \alpha^i \mod n \mid 0 \le i \le \emptyset(n) 1 \}$ $0 \le 1 \le$ 13 is prime => (6(n)=n-1=12

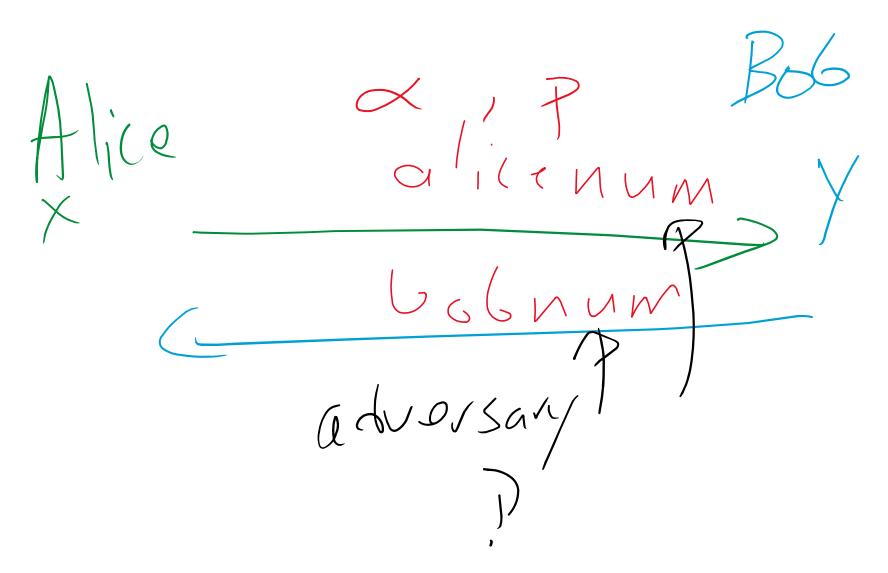
MOd

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



Now Back to Diffie-Hellman Key Exchange... $3 \propto -6$

- 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
 Protocol messages
 • Alice sends message to Bob: α^x mod p
 • Bob send message to Alice: α^y mod p
 (Step 1)
 606 num = 2^x mod p
 (Step 2)
- Protocol messages
- 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 $\alpha^x \mod p$ and computes the shared secret $K = \{\alpha^x \mod p\}^y \mod p = (\alpha^x)^y \mod p$
 - Alice receives α^{y} mod p and computes the shared secret $\mathbf{k} = (\alpha^{y} \mod p)^{k} \mod p = (\alpha^{y})^{k} \mod p$



Discrete Logarithm Robley T G_{1} X mod P 96 × 404 \$67, 56 (674) 12 31 Y=109

PINME PVIDE P 0 $\overline{}$ $\left(\right)$ 12 4091 2 704 Z ৾৵)

Diffie-Hellman Key Exchange Preserves

- 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_i in the future is not also given away
- This is not true of other schemes
 - e.g., in an <u>RSA</u> public-private key scheme
 - giving away the private key does compromise future communications