ECE 443/518 – Computer Cyber Security
Lecture 10 Diffie-Hellman and Man-in-the-Middle Attack

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

September 23, 2024

Outline

Reading Assignment

- This lecture: UC 8.1,8.5,13.3.1
- Next lecture: UC 10.1 – 10.3

Midterm Exam

- Lecture 1 $\sim$ Lecture 13, see Homework 1 and 2 for sample.
  - Points may be deducted if key steps are missing.
- Students registered for main campus section: Wed. 10/9, 11:25 AM – 12:40 PM, in class.
  - A physical calculator is allowed. Laptop or any other electronic device or calculator apps running on them are not allowed.
  - Closed book/notes. A letter-size page of cheat sheet is allowed.
- Online students may take the exam as above, or contact Charles Scott (scott@iit.edu) to make arrangement and confirm with me.
  - No make-up exam will be offered if you fail to do so.
- ADA Accommodations: contact Center for Disability Resource (disabilities@iit.edu)
- Emergency/extraordinary reasons for make-up midterm exams are accepted only with documented proof like docter's notes.

Outline

Perfect Forward Secrecy (PFS)

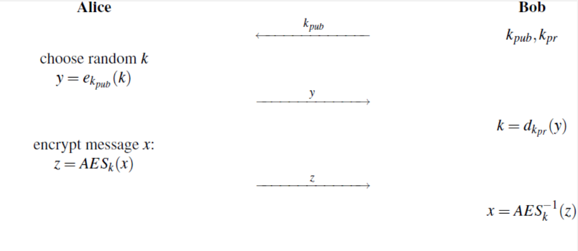


Fig. 6.5 Basic key transport protocol with AES as an example of a symmetric cipher

(Paar and Pelzl)

- Oscar, realizing there is no hope to factor every n for RSA, decided to build a machine to factor a few n's he/she might be interested of.
  - Oscar has recorded all communications encrypted using the simple hybrid protocol.
- How could Bob could protect k's if k_{pr} is compromised?
  - Will it help if Alice/Bob generates another RSA key-pair randomly per communication?

History of Diffie-Hellman Key Exchange

- 1976: created by Whitfield Diffie and Martin Hellman
  - First public-key algorithm in open literature.
- 1977: patent granted in US
- 2005: variants are included in NSA Suite B Cryptography
  - Together with AES and SHA-2

DHKE

Diffie–Hellman Key Exchange

Alice		Bob
choose $a = k_{pr,A} \in \{2, \dots, p-2\}$ compute $A = k_{pub,A} \equiv \alpha^a \bmod p$		choose $b = k_{pr,B} \in \{2, \dots, p-2\}$ compute $B = k_{pub,B} \equiv \alpha^b \bmod p$
	$\xrightarrow{k_{pub,A}=A}$	
	$\xleftarrow{k_{pub,B}=B}$	
$k_{AB} = k_{pub,B}^{k_{pr,A}} \equiv B^a \bmod p$		$k_{AB} = k_{pub,A}^{k_{pr,B}} \equiv A^b \bmod p$

(page 207, Paar and Pelzl)

- DHKE setup
  - A large prime p and an integer α chosen from $2, 3, \dots, p-2$.
  - Usually chosen/published by a well-known entity and used by a large group of people.
- Key exchange: upon completion, a shared secret k_{AB} is established between Alice and Bob.
  - Assume one of the public key is sent over an authentic channel.
- Time complexity: $O(N^3)$.

Example

- $p = 29, \alpha = 2$.
- Alice: $k_{pr,A} = 5$
  - $k_{pub,A} = 2^5 \bmod 29 = 3$
- Bob: $k_{pr,B} = 12$
  - $k_{pub,B} = 2^{12} \bmod 29 = 7$
- Alice: $k_{AB} = (k_{pub,B})^{k_{pr,A}} \bmod p = 7^5 \bmod 29 = 16$
  Bob: $k_{AB} = (k_{pub,A})^{k_{pr,B}} \bmod p = 3^{12} \bmod 29 = 16$

The Discrete Logarithm Problem

Given a prime number p, an integer $\alpha \in \{2, 3, \ldots, p-2\}$, and an integer B, solve for an integer b,

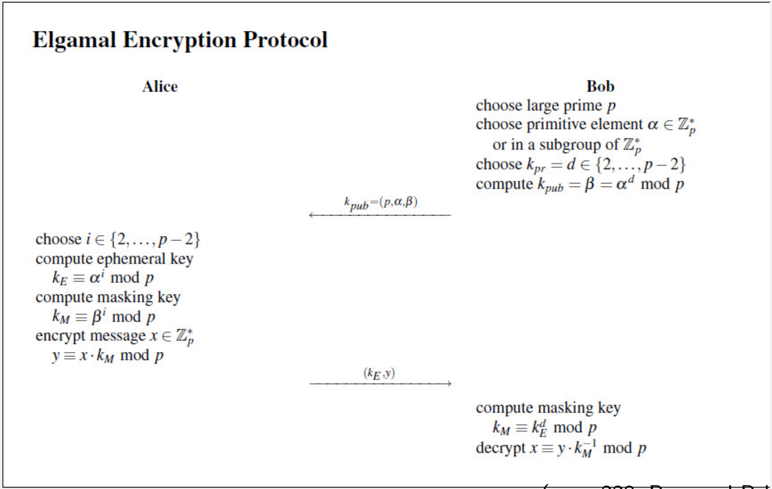
$$\alpha^b \equiv B \pmod{p}.$$

- A passive adversary may obtain $k_{pr,B}$ and then k_{AB}.
- Brute-force: compute $\alpha^k \bmod p$ for $k = 1, 2, \ldots, p-1$
  - Time complexity: $O(2^N N^2)$.
- Better algorithm exists, but still of exponential time.
- The Diffie-Hellman problem: compute $\alpha^{ab} \bmod p$ given $\alpha^a \bmod p$ and $\alpha^b \bmod p$ with α and p known.
  - It is unknown if this could be done without solving discrete logarithm first.
  - DHKE is believed to be secure for large enough N.
- Will Alice be able to learn Bob's private key?

The Elgamal Encryption Scheme

- An extension of DHKE for encryption.
- After successfully completing DHKE, Alice sends $y = k_{AB}x \bmod p$ to Bob.
  - Plaintext $x \in \{1, 2, \ldots, p-1\}$
  - Ciphertext $y \in \{1, 2, \ldots, p-1\}$
- Bob decrypts y by solving $k_{AB}x \equiv y \pmod{p}$ for x via EEA or other algorithms.
- Ephemeral keys: k_{AB} should be used only once.
  - A passive adversary who learned a pair of x and y could solve $k_{AB}x \equiv y \pmod{p}$ for k_{AB} and decrypts all other ciphertext with the same k_{AB}.

Elgamal Encryption Protocol



(page 228, Paar and Pelzl)

- Rearrange messages: Elgamal looks very similar to RSA
  - Assume Bob's public key is sent over an authentic channel.
  - Alice's message could be sent over an insecure channel.
  - Need padding for similar reasons as RSA.

DHKE vs. RSA

- Good alternatives of each other.
  - Their security depends on different problems that we don't know how to solve efficiently yet.
  - While DHKE was originally designed for key exchange, its variants can match with the functionalities provided by RSA.
- Both DHKE and RSA may need an authentic channel for communicating a public key.
- In practice, both DHKE and RSA use keys a few thousand bits long to be secure.
- DHKE can be generalized to other mathematical structures.
  - E.g. elliptic-curve cryptography (ECC), which requires much less bits to achieve same level of security as DHKE, and is widely adopted currently.

Outline

The Authentic Channel

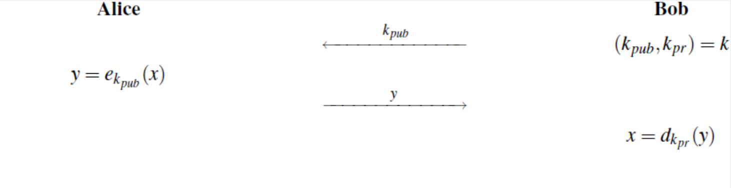


Fig. 6.4 Basic protocol for public-key encryption

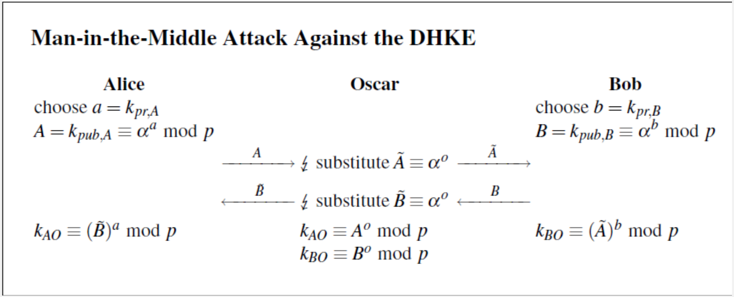
(Paar and Pelzl)

- We do see how RSA and DHKE (Elgamal) both use the above protocol for public key encryption.
- Both require Alice to receive Bob's public key on an authentic channel.
  - What if not?

Man-in-the-Middle Attack

- Assume Bob's public key $k_{pub,B}$ is sent through an insecure channel.
- Oscar the active adversary replaces $k_{pub,B}$ that Alice receives.
  - With Oscar's public key $k_{pub,O}$.
- Alice receives $k_{pub,O}$ and encrypts x as $y = e_{k_{pub,O}}(x)$.
- Oscar replaces y that Bob receives.
  - With $y' = e_{k_{pub,B}}(x)$.
  - Note that Oscar simply decrypts y to obtain x since y is encrypted with $k_{pub,O}$: $x = d_{k_{pr,O}}(y)$.
- Man-in-the-Middle: Oscar sits between Alice and Bob, and replaces all messages on either direction.
  - Neither Alice and Bob will be able to detect it!

Man-in-the-Middle and DHKE



(Paar and Pelzl)

- This attack also applies to the original DHKE assuming both Alice and Bob's public keys are not sent via an authentic channel.
  - Oscar then have two secret keys, one with Alice and one with Bob, that can be used for any following communications.
- What if, as originally assumed, one of Alice and Bob's public keys is sent via an authentic channel?
- Does man-in-the-middle attack apply to symmetric ciphers?

Identity

- The problem of man-in-the-middle attack is with identity.
  - Alice sees Oscar as Bob.
  - Bob sees Oscar as Alice.
- The authentic channel authenticates that a public key belongs to a particular identity.
  - To create an authentic channel, we need to study how to establish identity – who is Bob?
- Can we establish identity without the authentic channel?
  - Yes if the public key is the identity, but how?
  - Note that in a successful man-in-the-middle attack, communications between Alice and Oscar is secure against any third party including Bob, and communications between Oscar and Bob is secure against any third party including Alice.

Summary

- DHKE
  - Setup: prime p, $\alpha \in \{2, 3, \ldots, p-2\}$.
  - Alice: $k_{pr,A}$, publish $k_{pub,A} = \alpha^{k_{pr,A}} \bmod p$
  - Bob: $k_{pr,B}$, publish $k_{pub,B} = \alpha^{k_{pr,B}} \bmod p$
  - Alice and Bob: $k_{AB} \equiv (k_{pub,B})^{k_{pr,A}} \equiv (k_{pub,A})^{k_{pr,B}} \pmod{p}$
  - Assumption: Oscar cannot solve $\alpha^b \equiv B \pmod{p}$ for b in polynomial time.
- Man-in-the-Middle attack