Cryptography and Network Security

DIFFIE HELLMAN KEY EXCHANGE

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	6 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Diffie-Hellman protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Introduction

Amongst the tribes of Central Australia every man, woman, and child has a secret or sacred name which is bestowed by the older men upon him or her soon after birth, and which is known to none but the fully initiated members of the group. This secret name is never mentioned except upon the most solemn occasions; to utter it in the hearing of men of another group would be a most serious breach of tribal custom. When mentioned at all, the name is spoken only in a whisper, and not until the most elaborate precautions have been taken that it shall be heard by no one but members of the group. The native thinks that a stranger knowing his secret name would have special power to work him ill by means of magic.

—The Golden Bough, Sir James George Frazer

Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Diffie-Hellman Key Exchange

- first public-key type scheme proposed
- by Diffie & Hellman in 1976 along with the exposition of public key concepts
  - note: now know that Williamson (UK CESG) secretly proposed the concept in 1970
- is a practical method for public exchange of a secret key
- used in a number of commercial products

Diffie-Hellman Key Exchange

- a public-key distribution scheme
  - cannot be used to exchange an arbitrary message
  - rather it can establish a common key
  - known only to the two participants
- value of key depends on the participants (and their private and public key information)
- based on exponentiation in a finite (Galois) field (modulo a prime or a polynomial) - easy
- security relies on the difficulty of computing discrete logarithms (similar to factoring) – hard

Diffie-Hellman Setup

- all users agree on global parameters:
  - large prime integer or polynomial q
  - a being a primitive root mod q
- each user (eg. A) generates their key
  - chooses a secret key (number): $x_A < q$
  - compute their **public key**: $y_A = a^{x_A} \bmod q$
- each user makes public that key y_A

Diffie-Hellman Key Exchange

- shared session key for users A & B is K_{AB}:

  $K_{AB} = a^{x_A.x_B} \bmod q$

  $= y_A^{x_B} \bmod q$ (which **B** can compute)

  $= y_B^{x_A} \bmod q$ (which **A** can compute)
- K_{AB} is used as session key in private-key encryption scheme between Alice and Bob
- if Alice and Bob subsequently communicate, they will have the **same** key as before, unless they choose new public-keys
- attacker needs an x, must solve discrete log

Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Diffie-Hellman Example

- users Alice & Bob who wish to swap keys:
- agree on prime q=353 and a=3
- select random secret keys:
  - A chooses x_A=97, B chooses x_B=233
- compute respective public keys:
  - $y_A = 3^{97} \bmod 353 = 40$ (Alice)
  - $y_B = 3^{233} \bmod 353 = 248$ (Bob)
- compute shared session key as:
  - $K_{AB} = y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)
  - $K_{AB} = y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

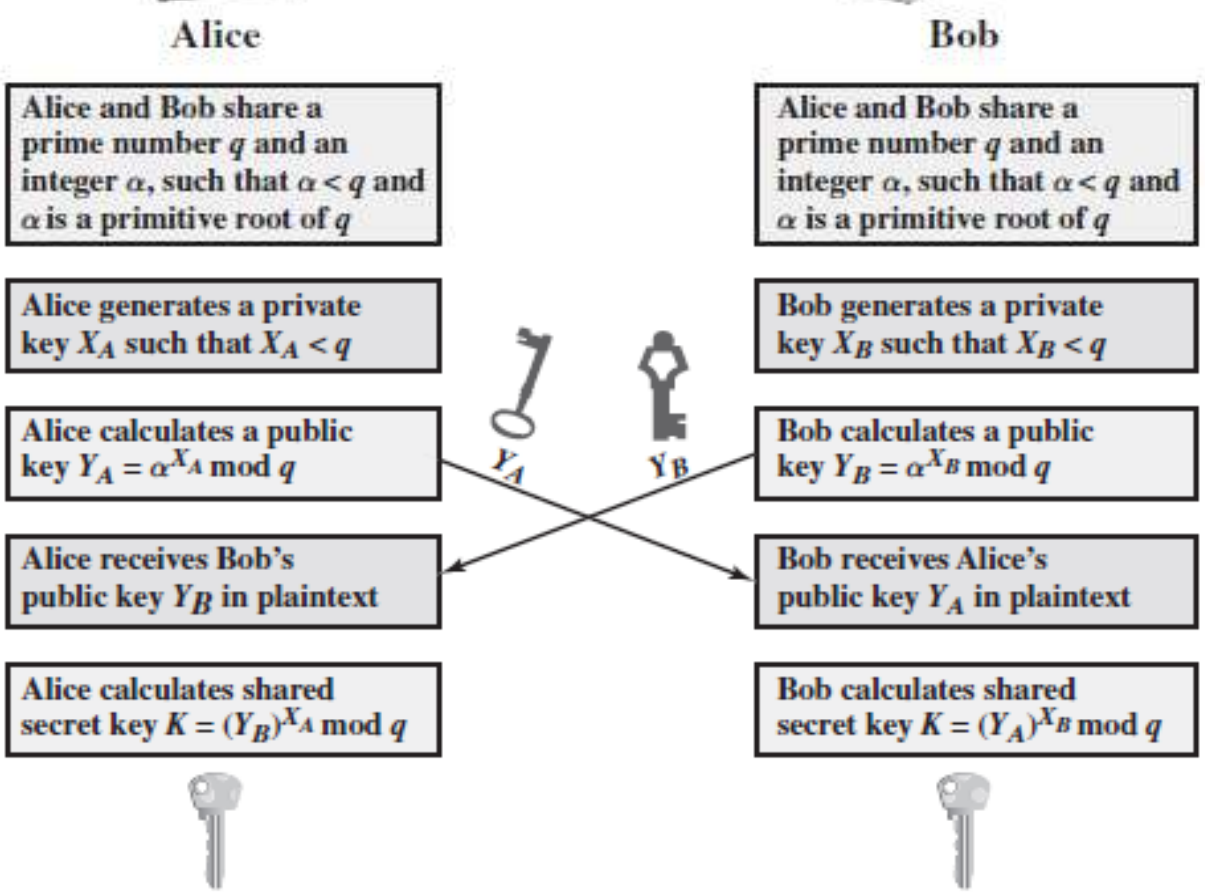
Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Key Exchange Protocols

- users could create random private/public D-H keys each time they communicate
- users could create a known private/public D-H key and publish in a directory, then consulted and used to securely communicate with them
- both of these are vulnerable to a Man-in-the-Middle Attack
- authentication of the keys is needed

Key Exchange Protocols



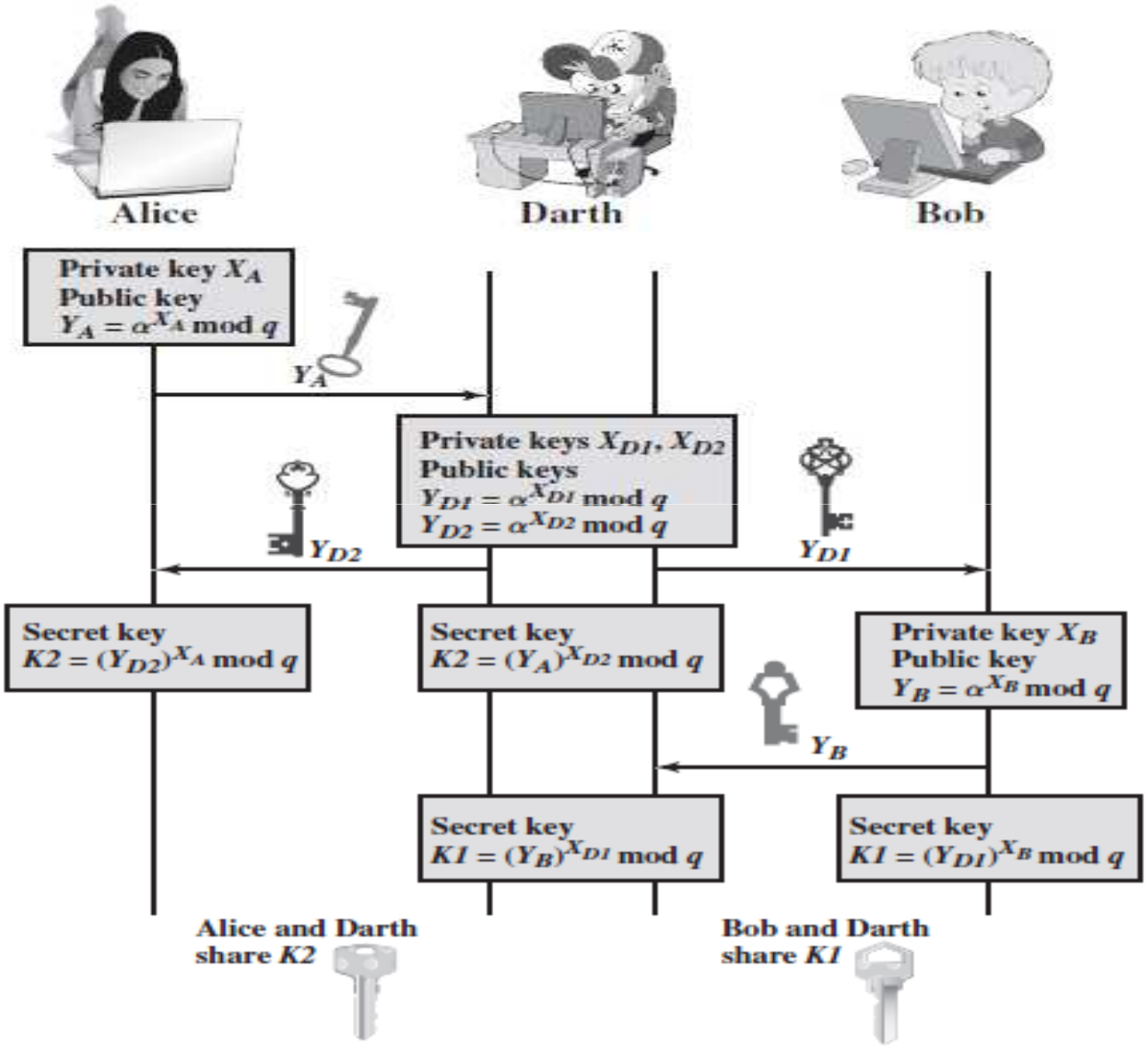
Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Man-in-the-Middle Attack

1. Darth prepares by creating two private / public keys
2. Alice transmits her public key to Bob
3. Darth intercepts this and transmits his first public key to Bob. Darth also calculates a shared key with Alice
4. Bob receives the public key and calculates the shared key (with Darth instead of Alice)
5. Bob transmits his public key to Alice
6. Darth intercepts this and transmits his second public key to Alice. Darth calculates a shared key with Bob
7. Alice receives the key and calculates the shared key (with Darth instead of Bob)
8. Darth can then intercept, decrypt, re-encrypt, forward all messages between Alice & Bob

Man-in-the-Middle Attack



Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Summary

- Define Diffie-Hellman key exchange
- Understand the man-in-the-middle attack

Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

Test your understanding

1. Briefly explain Diffie-Hellman key exchange.
2. Users A and B use the Diffie-Hellman key exchange technique with a common prime *q = 71 and a primitive root a = 7.*
   a. If user A has private key *XA = 5, what is A's public key YA?*
   b. If user B has private key *XB = 12, what is B's public key YB?*
   c. What is the shared secret key?
3. Consider a Diffie-Hellman scheme with a common prime *q = 11 and a primitive root* a = 2.
   a. Show that 2 is a primitive root of 11.
   b. If user A has public key *YA = 9, what is A's private key XA?*
   c. If user B has public key *YB = 3, what is the secret key K shared with A?*

Agenda

- Introduction
- Diffie-Hellman key exchange
- Diffie-Hellman example
- Key exchange protocol
- Man-in-the-middle attack
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.