

DIFFIE-HELLMAN KEY EXCHANGE CONT.

Lecture 8a

COMPSCI 726

Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

August 4, 2021

DISCRETE LOG PROBLEM



- Let g be a generator of group Z_n^* and let $y \in Z_n^* = \{g^1, g^2, \dots, g^{n-1}\} = \{1, 2, \dots, n-1\}$
- Given n , g , and y , find an integer x such that $y \equiv g^x \pmod{n}$
- Example
 - Given $n = 7$, $g = 5$, and $y = 2$
 - Find x , where $2 \equiv 5^x \pmod{7}$
- Typically, n is a very large prime!



DIFFIE-HELLMAN KEYS



- Let g is a generator of group Z_n^*
- Public parameter: g, n
- Private key: $x \in (1, 2, \dots, n-1)$
- Public key: $g^x \pmod n$

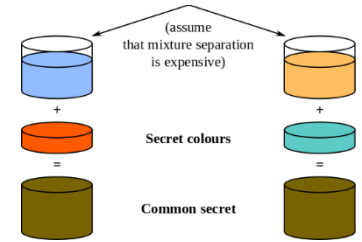
- Example
 - Let $g = 5$ and $n = 7$
 - Private key: $x = 4$
 - Public key: $5^4 \pmod 7 \equiv 5^2 \cdot 5^2 \pmod 7$
 $\equiv 4 \cdot 4 \pmod 7 \equiv 16 \pmod 7 \equiv 2$

DIFFIE-HELLMAN KEY EXCHANGE



- A public key distribution scheme to establish session keys
- Invented by Diffie and Hellman in 1976
- First public key cryptosystem
- Used in a number of commercial products
- Security relies on difficulty of computing discrete log, which is hard
- It is vulnerable to Man-in-the-Middle (MitM) attack

DIFFIE-HELLMAN KEY EXCHANGE



Alice (x)



g^x

g^y

Bob (y)



$$k \equiv (g^y)^x \equiv g^{xy} \pmod{n}$$

$$k \equiv (g^x)^y \equiv g^{xy} \pmod{n}$$

- A key (k) has been established
- Alice and Bob can encrypt messages using this key

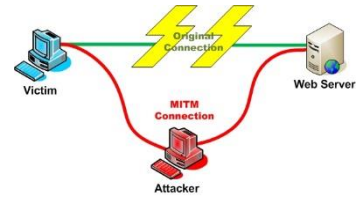
Enc(k, m1)



Enc(k, m2)



MAN-IN-THE-MIDDLE ATTACK



Alice (x)

Darth (z)

Bob (y)



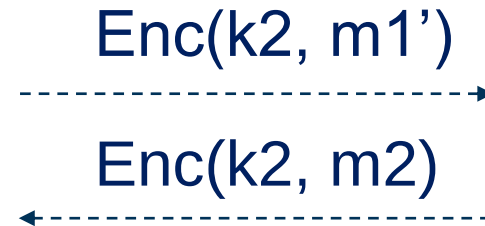
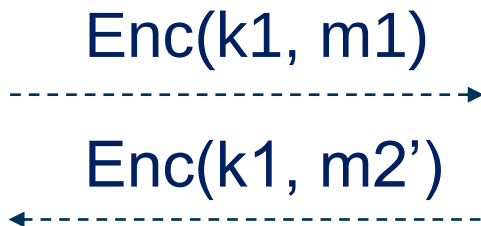
$$k1 \equiv g^{xz}$$

$$k1 \equiv g^{xz}$$

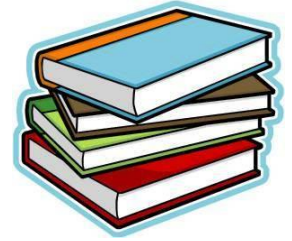
$$k2 \equiv g^{yz}$$

$$k2 \equiv g^{yz}$$

- Keys have been established
- Messages could be encrypted using established keys



RESOURCES



- Read Chapter 3 of
Network Security Essentials – Applications and Standards
Fourth Edition
William Stallings
Prentice Hall
ISBN 0-13-706792-5



Questions?

Thanks for your attention!