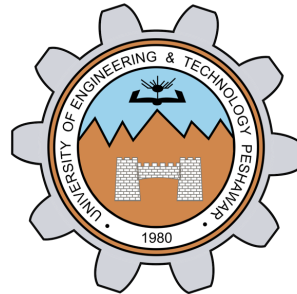


# Computer Security

## Lecture 10: Diffie-Hellman Key Exchange

**Prof. Dr. Sadeeq Jan**

Department of Computer Systems Engineering  
University of Engineering and Technology Peshawar



# Diffie-Hellman Key Exchange

- Diffie-Hellman Key Exchange

# Diffie-Hellman Key Exchange



- First PKC offered by Diffie and Hellman in 1976
- still in commercial use
- purpose is secure key-exchange
  - actually key “agreement”
  - both parties agree on a session key without releasing this key to a third party
    - to be used for further communication using symmetric crypto
- Security is in the hardness of the discrete logarithm problem
  - given  $g^x \bmod p$ ,  $g$  and  $p$ , it is computationally infeasible to find out  $x$  if  $p$  is large enough prime number

# Cappuccino Recipe

Easy



Hard

# Diffie-Hellman Key exchange



- Requires two large numbers, one prime ( $P$ ), and ( $G$ ), a primitive root of  $P$

## 3 is a primitive root of 5:

If the set of remainders in the third column reproduces the set of integers in the first (the order need not be identical), then 3 is a primitive root of 5. It looks like 3 is indeed a primitive root of 5.

n	$3^n$	$3^n \bmod 5$
1	3	3
2	9	4
3	27	2
4	81	1

## 4 on the other hand is not,

because we won't get the values 1 through 4 when we repeat the above process.

x	$4^x$	$4^x \bmod 5$
1	4	4
2	16	1
3	64	4
4	256	1

# Implementation



- P and G are both publicly available numbers
  - P is at least 512 bits
- Users pick private values a and b
- Compute public values
  - $A = g^a \bmod p$
  - $B = g^b \bmod p$
- Public values A and B are exchanged



- Both users Compute shared, private key
  - $s = B^a \bmod p$
  - $s = A^b \bmod p$
- Algebraically it can be shown that both s are equal.
  - Thus, Users now have a symmetric secret key to encrypt

# Example



- Alice and Bob agree to use a prime number  $p=23$  and base  $g=5$ .
- Alice chooses a secret integer  $a=6$ , then sends Bob  $A = g^a \bmod p$ 
  - $A = 5^6 \bmod 23$
  - $A = 15,625 \bmod 23$
  - $A = 8$
- Bob chooses a secret integer  $b=15$ , then sends Alice  $B = g^b \bmod p$ 
  - $B = 5^{15} \bmod 23$
  - $B = 30,517,578,125 \bmod 23$
  - $B = 19$
- Alice computes  $s = B^a \bmod p$ 
  - $s = 19^6 \bmod 23$
  - $s = 47,045,881 \bmod 23$
  - $s = 2$

# Example-contd..



- Bob computes  $s = A^b \bmod p$ 
  - $s = 8^{15} \bmod 23$
  - $s = 35,184,372,088,832 \bmod 23$
  - $s = 2$
- Alice and Bob now share a secret:  $s = 2$ . This is because  $6 \cdot 15$  is the same as  $15 \cdot 6$ . So somebody who had known both these private integers might also have calculated  $s$  as follows:
  - $s = 5^{6 \cdot 15} \bmod 23$
  - $s = 5^{15 \cdot 6} \bmod 23$
  - $s = 5^{90} \bmod 23$
  - $s = 807,793,566,946,316,088,741,610,050,849,573,099,185,363,389,551,639,556,884,765,625 \bmod 23$
  - $s = 2$

- Both Alice and Bob have arrived at the same value, because  $(g^a)^b$  and  $(g^b)^a$  are equal mod  $p$ . Note that only  $a$ ,  $b$  and  $g^{ab} = g^{ba} \bmod p$  are kept secret. All the other values –  $p$ ,  $g$ ,  $g^a \bmod p$ , and  $g^b \bmod p$  – are sent in the clear

# Example - Diffie-Hellman Key exchange

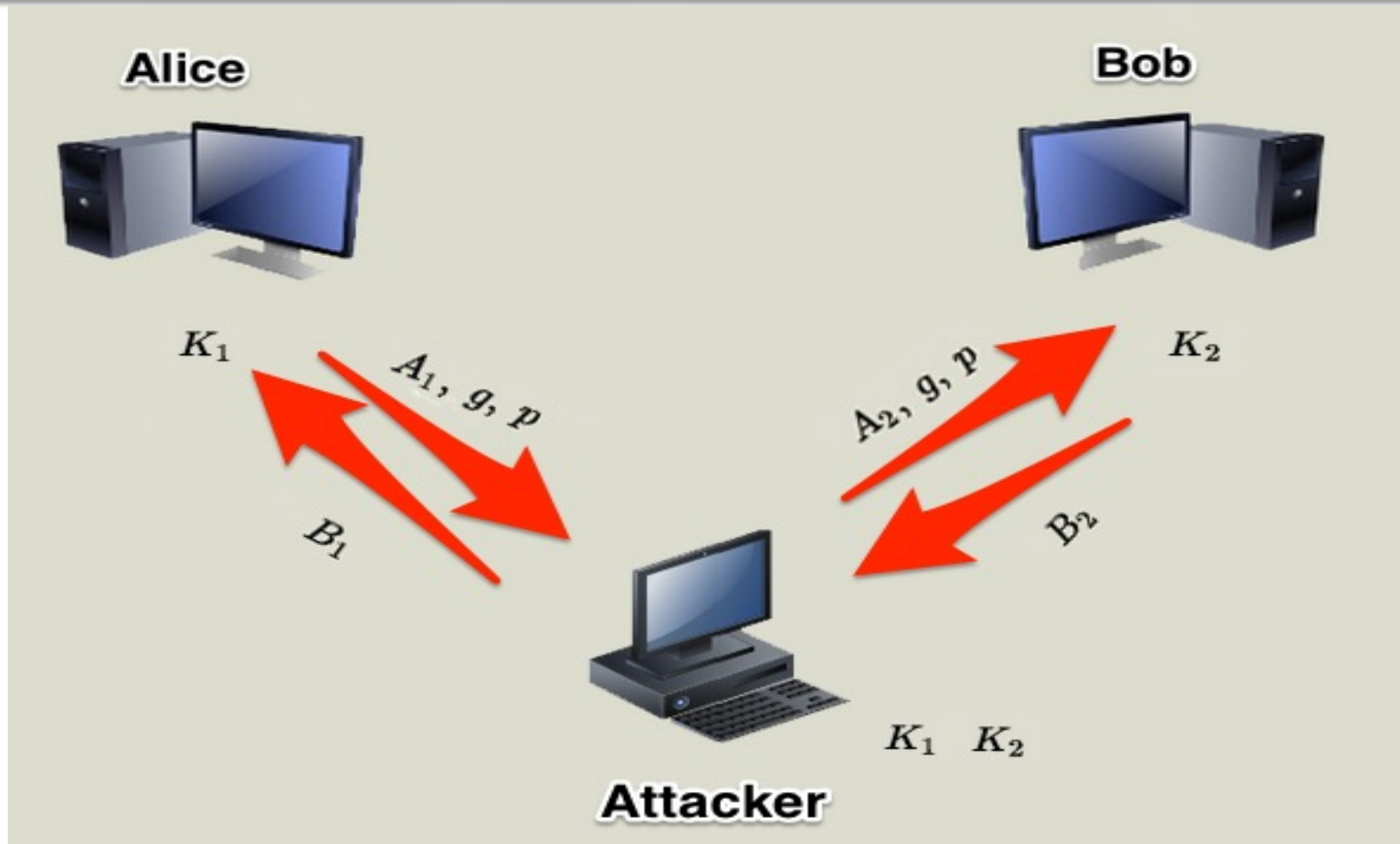
	Alice	Evil Eve	Bob
	Alice and Bob exchange a Prime (P) and a Generator (G) in clear text, such that $P > G$ and G is Primitive Root of P $G = 7, P = 11$		Alice and Bob exchange a Prime (P) and a Generator (G) in clear text, such that $P > G$ and G is Primitive Root of P $G = 7, P = 11$
Step 1	Alice generates a random number: $X_A$ $X_A = 6$ (Secret)		Bob generates a random number: $X_B$ $X_B = 9$ (Secret)
Step 2	$Y_A = G^{X_A} \pmod{P}$ $Y_A = 7^6 \pmod{11}$ $Y_A = 4$		$Y_B = G^{X_B} \pmod{P}$ $Y_B = 7^9 \pmod{11}$ $Y_B = 8$
Step 3	Alice receives $Y_B = 8$ in clear-text	Evil Eve sees $Y_A = 4, Y_B = 8$	Bob receives $Y_A = 4$ in clear-text
Step 4	Secret Key = $Y_B^{X_A} \pmod{P}$ Secret Key = $8^6 \pmod{11}$ 🔑 Secret Key = 3		Secret Key = $Y_A^{X_B} \pmod{P}$ Secret Key = $4^9 \pmod{11}$ 🔑 Secret Key = 3

# Diffie-Hellman Example



- users Alice & Bob who wish to swap keys:
- agree on prime  $p=353$  and  $g=3$
- select random secret keys:
  - A chooses  $x_A=97$ , B chooses  $x_B=233$
- compute 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)

# D-H Key Exchange – Man in the middle attack



**END**