Information and Cyber Security

Assignment No.7

R (2)	C (4)	V (2)	T (2)	Total (10)	Dated Sign

7.1 Title:

Implementation of Diffie-Hellman key Exchange (DH)

7.2 Problem Definition:

Implementation of Diffie-Hellman key Exchange (DH)

7.3 Prerequisite:

Basics of Computer Networking and Python

7.4 Software Requirements:

Python 3

7.5 Hardware Requirements:

PIV, 2GB RAM, 500 GB HDD

7.6 Learning Objectives:

Learn Diffie-Hellman key Exchange (DH)

7.7 Outcomes:

After completion of this assignment students are able to understand the Diffie-Hellman key Exchange

7.8 Theory Concepts:

7.8.1 Diffie-Hellman key Exchange (DH)

In the mid- 1970's, Whitefield Diffie, a student at the Stanford University met with Martin Hellman, his professor &the two began to think about it. After some research & complicated mathematical analysis, they came up with the idea of AKC. Many experts believe that this development is the first & perhaps the only truly revolutionary concept in the history of cryptography.

7.8.2 Silent Features of Diffie-Hellman key Exchange (DH)

1. Developed to address shortfalls of *key distribution* in symmetric key distribution.
2. A *key exchange algorithm*, not an encryption algorithm
3. Allows two users to share a *secret key* securely over a public network
4. Once the key has been shared Then both parties can use it to encrypt and decrypt messages using symmetric cryptography
5. Algorithm is based on "difficulty of calculating discrete logarithms in a finite field"
6. These keys are mathematically related to each other.
7. ''Using the public key of users, the session key is generated without transmitting the private key of the users.''

7.8.3 Diffie-Hellman Key Exchange/Agreement Algorithm with Example

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

   Let $n = 11$, $g = 7$.

2. Alice chooses another large random number x, and calculates A such that:
   $A = g^x \bmod n$

   Let $x = 3$. Then, we have, $A = 7^3 \bmod 11 = 343 \bmod 11 = 2$.

3. Alice sends the number A to Bob.

   Alice sends 2 to Bob.

4. Bob independently chooses another large random integer y and calculates B such that:
   $B = g^y \bmod n$

   Let $y = 6$. Then, we have, $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$.

5. Bob sends the number B to Alice.

   Bob sends 4 to Alice.

6. A now computes the secret key K1 as follows:
   $K1 = B^x \bmod n$

   We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9$.

7. B now computes the secret key K2 as follows:
   $K2 = A^y \bmod n$

   We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9$.

7.8.4 Diffie-Hellman Key exchange

1. Public values:
   - large prime p, generator g (primitive root of p)
2. Alice has secret value x, Bob has secret y
3. Discrete logarithm problem: given x, g, and n, find A
4. A $\rightarrow$ B: g^x (mod n)
5. B $\rightarrow$ A: g^y (mod n)
6. Bob computes $(g^x)^y = g^{xy}$(mod n)
7. Alice computes $(g^y)^x = g^{xy}$ (mod n)
8. Symmetric key= g^{xy} (mod n)

7.8.5 Limitation: Vulnerable to “man in the middle” attacks*

7.8.5.1 Man-in-the-Middle Attack:

Alice	Tom	Bob
n = 11, g = 7	n = 11, g = 7	n = 11, g = 7

Figure 7.1 Man-in-the-Middle Attack Part-I

Alice	Tom	Bob
x = 3	x = 8, y = 6	y = 9

Figure 7.2 Man-in-the-Middle Attack Part-II

Alice	Tom	Bob
$A = g^x \bmod n$	$A = g^x \bmod n$	$B = g^y \bmod n$
$= 7^3 \bmod 11$	$= 7^8 \bmod 11$	$= 7^9 \bmod 11$
$= 343 \bmod 11$	$= 5764801 \bmod 11$	$= 40353607 \bmod 11$
$= 2$	$= 9$	$= 8$
	$B = g^y \bmod n$	
	$= 7^6 \bmod 11$	
	$= 117649 \bmod 11$	
	$= 4$	

Figure 7.3 Man-in-the-Middle Attack Part-III

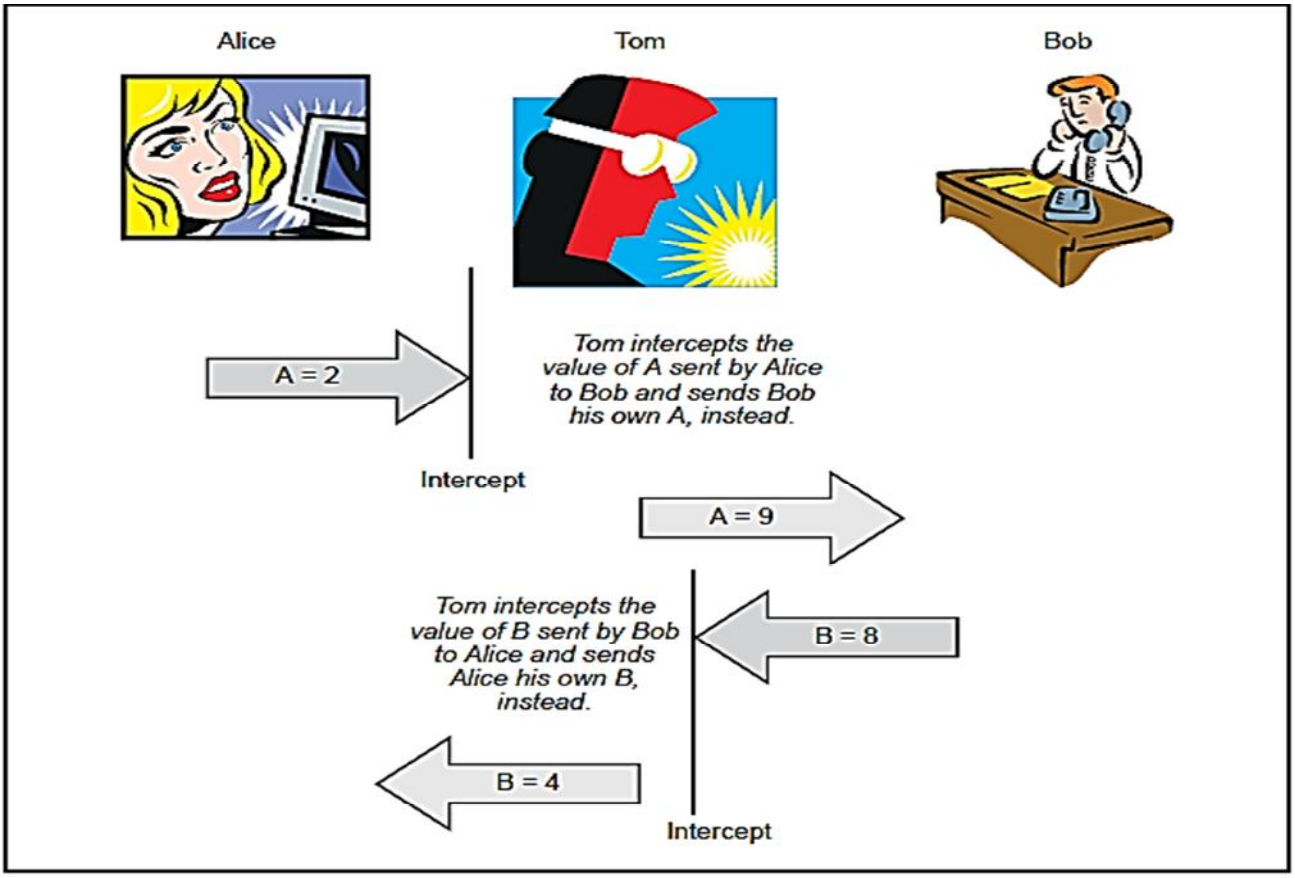

Figure 7.4 Man-in-the-Middle Attack Part-IV

Alice	Tom	Bob
A = 2, B = 4*	A = 2, B = 8	A = 9*, B = 8

(Note: * indicates that these are the values after Tom hijacked and changed them.)

Figure 7.5 Man-in-the-Middle Attack Part-V

Alice	Tom	Bob
$K1 = B^x \bmod n$	$K1 = B^x \bmod n$	$K2 = A^y \bmod n$
$= 4^3 \bmod 11$	$= 8^8 \bmod 11$	$= 9^9 \bmod 11$
$= 64 \bmod 11$	$= 16777216 \bmod 11$	$= 387420489 \bmod 11$
$= 9$	$= 5$	$= 5$
	$K2 = A^y \bmod n$	
	$= 2^6 \bmod 11$	
	$= 64 \bmod 11$	
	$= 9$	

Figure 7.6 Man-in-the-Middle Attack Part-VI

7.8.6 Preventing a Man-in-the-Middle Attack with Hashing

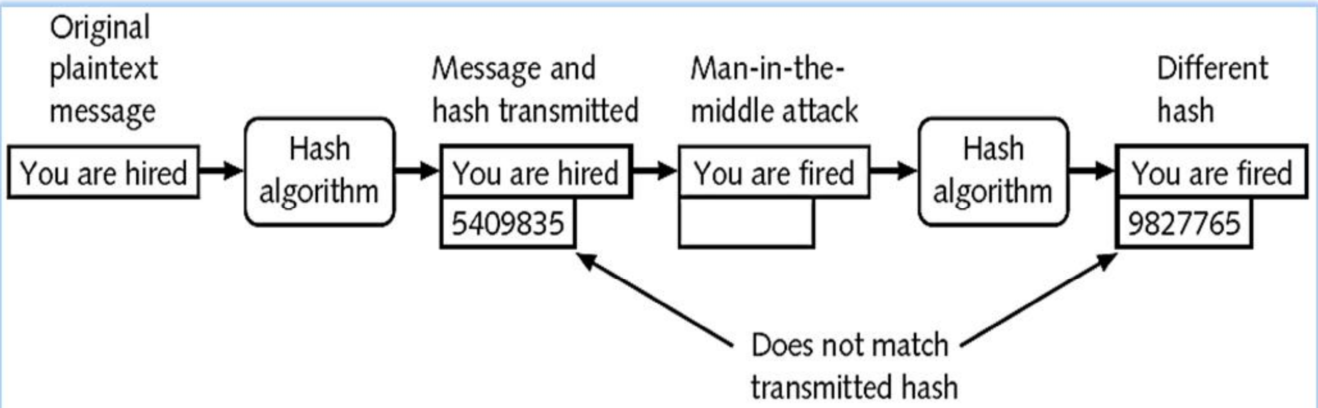

Figure 11-4 Man-in-the-middle attack defeated by hashing

Conclusion: Thus we have studied and implement Diffie-Hellmen key exchange algorithm and how to prevent Man-in-the-Middle Attack

Oral Questions

1. Explain "Diffie-Hellmen key exchange algorithm with suitable example
2. What is Man in the middle attack?
3. How to Preventing a Man-in Middle Attack?