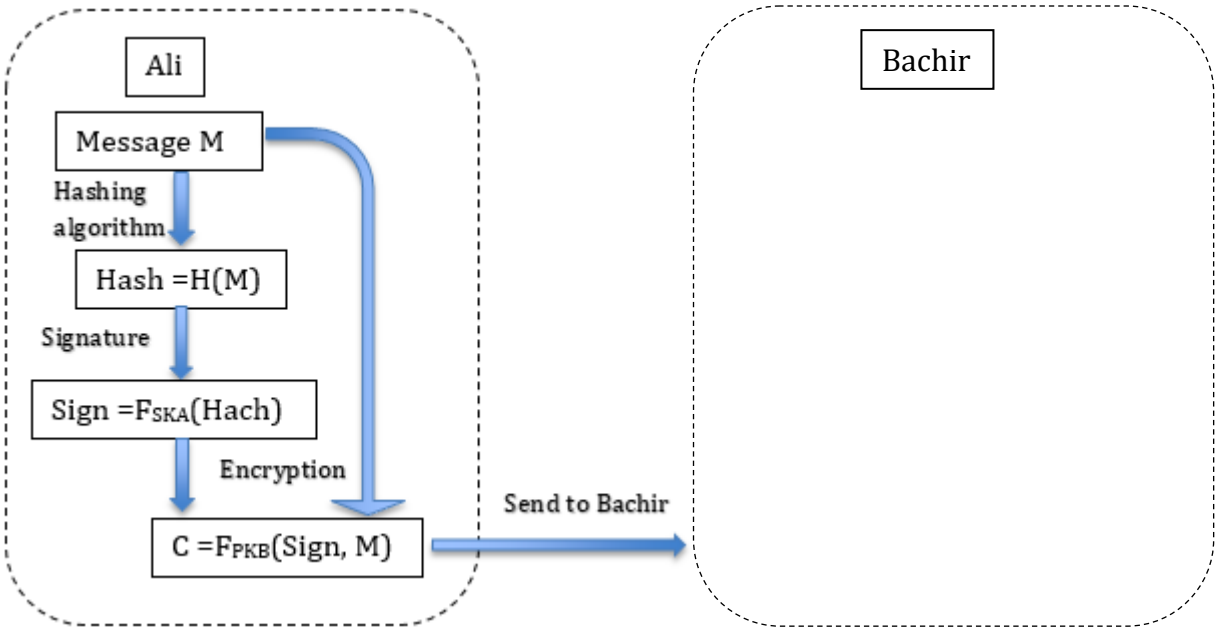
University of Echahid Hamma Lakhdar
Faculty of Exact sciences
Level: 1st year IoT&Cyber Security Master degree

Module: Information Security.
Date: 07-01- 2024.
Duration: 1 hr, 30 mins.

Final Exam

Exercise 1:

Ali and Bachir use asymmetric encryption, hash functions, and digital signatures to ensure secure message exchange. Each person possesses a pair of keys, consisting of a public key (PK_A, PK_B) and a private key (SK_A, SK_B). Ali follows a specific process to send a secure message.



1. Complete the figure by illustrating the process that Bachir follows when he receives the message.
2. What security services are provided in the preceding exchange? Specify the corresponding step for each service.
3. Explain, in a diagram, how a third person can potentially attack the exchange of public keys at the beginning.
4. What is the solution to prevent this attack, and how can it be implemented?
5. The security protocols IPSec and SSL/TLS utilize asymmetric encryption. Specify the TCP/IP layer in which these protocols operate

Exercise 2:

1. In a website, a user introduces his name and password on a **login** webpage. If correct, his name will be displayed on a **welcome** page.
   - Draw a graphical interface for the two webpages: login and welcome.
2. The user introduces the following url in the address field of a browser: http://www.example.com/welcome.php?name=<script>alert("LEAVE THIS PAGE! YOU ARE BEING HACKED!");</script>
   - Draw what the web site will show to the user.
3. Suppose that we have the following code fragment:

```
txtUserId=getRequestString("UserId"); // UserId is a text box.
```

txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;

- How to perform a SQL Injection attack to show all rows from the Users Table?
- How to perform a SQL Injection attack to delete the Students Table?

Exercise 3:

IPSec protocol uses two protocols and two operating modes. Complete the following table that describes the components of an IP packet in each case where **{...}**: Authenticated. **[...]** : Encrypted.

Protocols	Modes	
	Transport	…….
……	……	……
ESP	……	**{**New IP Header - ESP Header- **[**original IP header – Data- ESP trailer**]** – Authentication Data**}**.

Exercise 4:

Give a brief explanation of the following attack: ARP Poisoning, Smurf DDos Attack, Stack buffer overflow.

التمرين 1:

يريد علي وبشير إجراء تبادل آمن للرسائل باستخدام التشفير غير التناظري.

1- أكمل الشكل بتوضيح الخطوات اللازمة التي يتبعها بشير عند استقبال الرسالة.
2- ماهي خدمات الأمان التي يوفرها هذا التبادل؟ حدد لكل خدمة الخطوة التي توفرها.
3- اشرح باستخدام مخطط كيف لشخص ثالث مهاجمة تبادل المفاتيح العامة في البداية.
4- ما هو الحل لتفادي الهجوم؟
5- حدد الطبقات التي يعمل بها بروتوكولين IPSec, TLS/SSL

التمرين 2:

1- في موقع ويب يقوم المستخدم بإدخال الاسم وكلمة المرور في صفحة **login** إذا كانت المعلومات صحيحة يتم عرض اسمه في صفحة الترحيب (**welcome**). ارسم الواجهتين **login** و **welcome**
2- ارسم الواجهة التي يعرضها الموقع عند إدخال العنوان http المذكور.
3- -كيف يتم هجوم SQL Injection لاستظهار جميع أسطر الجدول Users – الهجوم الثاني لحذف الجدول Students

التمرين 3:

أكمل الجدول الذي يظهر مكونات IP Packet لكل حالة من حالات عمل بروتوكول IPSec

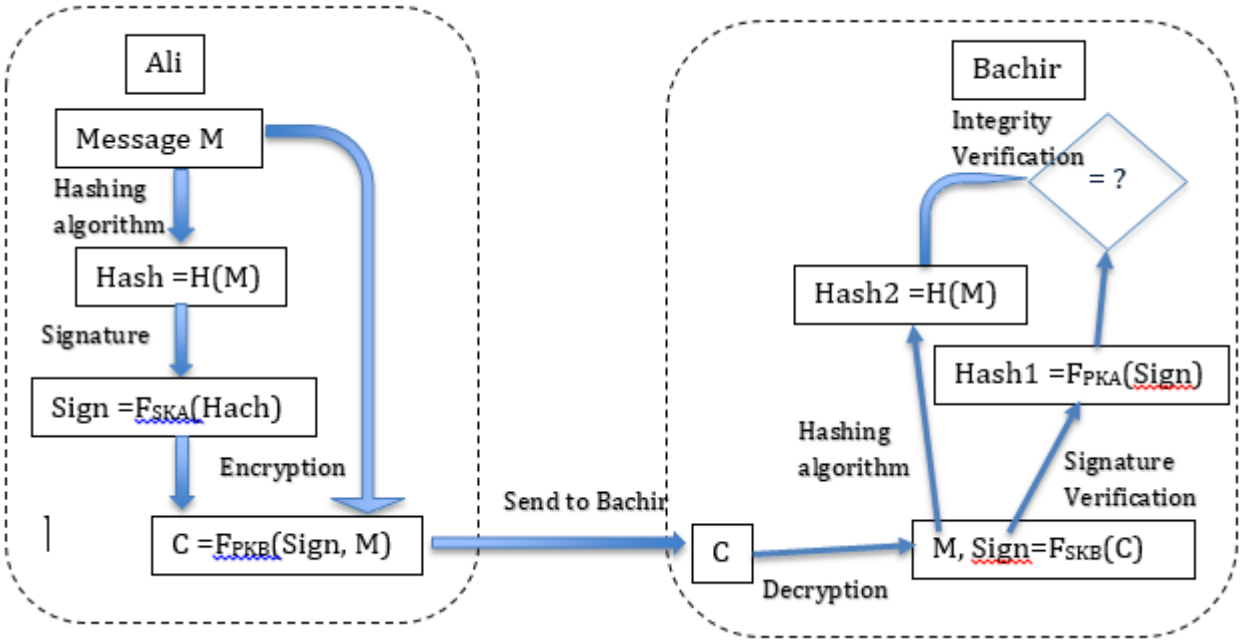
التمرين 4:

أعطي شرح مختصر للهجمات التالية: Stack buffer Overflow, ARP Poisoning, Smurfing

Information security final Exam correction

Exercise 2:

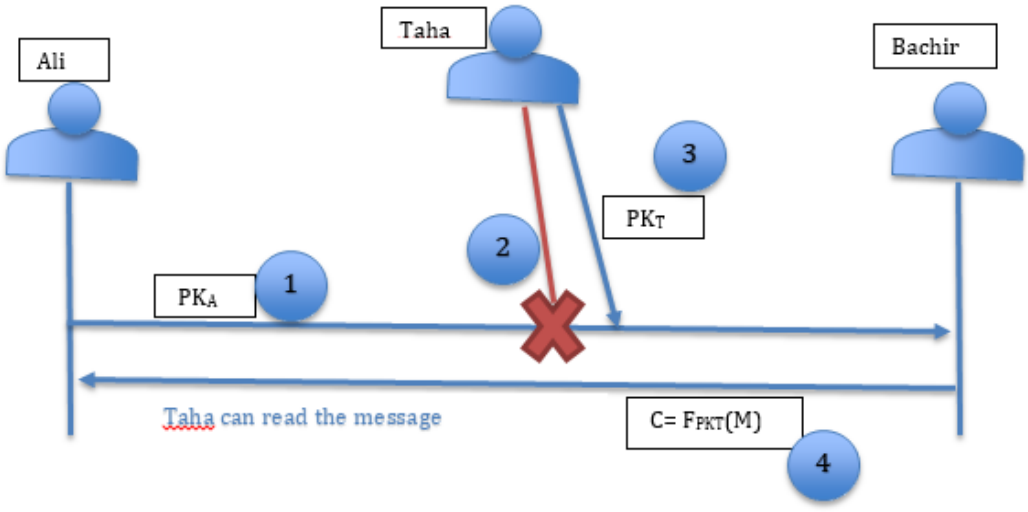
1- Complete the figure by illustrating the process that Bachir follows when he receives the message.



2- What security services are provided in the preceding exchange? Specify the corresponding step for each service.
The security services provided by this exchange are

Security services	Step
Authentication	Digital signature
Non repudiation	Digital signature
Confidentiality	Encryption
Integrity	Hashing algorithm

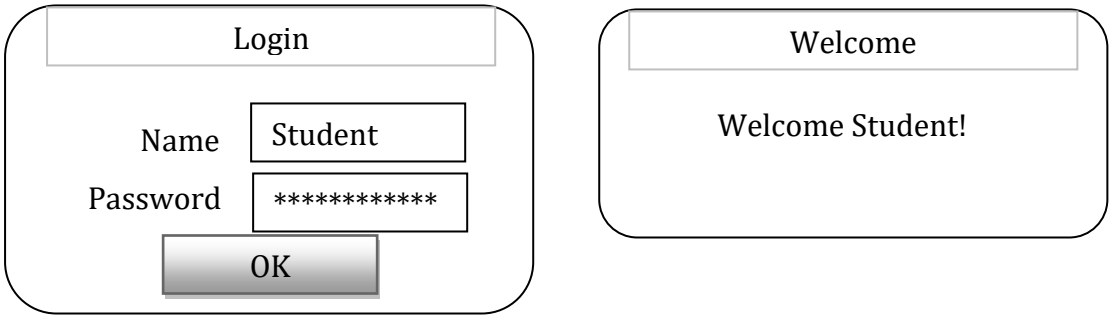
3- Explain, in a diagram, how a third person can potentially attack the exchange of public keys at the beginning.



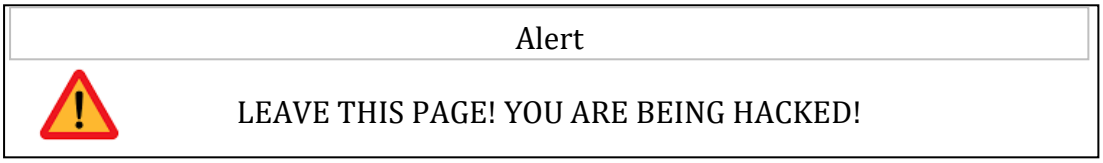
4- What is the solution to prevent this attack, and how can it be implemented?
Digital certificate signed by a trusted third party authority.
5- The security protocols IPSec and SSL/TLS utilize asymmetric encryption. Specify the TCP/IP layer in which these protocols operate.
IPSec : Internet layer.
SSL/TLS: Application layer.

Exercise 2:

1. In a website, a user introduces his name and password on a **login** webpage. If correct, his name will be displayed on a **welcome** page.
Draw a graphical interface for the two webpages: login and welcome.



2. The user introduces the following url in the address field of a browser: http://www.example.com/welcome.php?name=<script>alert("LEAVE THIS PAGE! YOU ARE BEING HACKED!");</script>
   - Draw what the web site will show to the user.



3. Suppose that we have the following code fragment:

```
txtUserId=getRequestString("UserId"); // UserId is a text box.

txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

   - How to perform a SQL Injection attack to show all rows from the Users Table?
   Write **UserId:** 105 OR 1=1 then, the SQL statement will look like this:
   SELECT * FROM Users WHERE UserId = 105 OR 1=1;
   - How to perform a SQL Injection attack to delete the Students Table?

Write User id: **105; DROP TABLE Students;**
The valid SQL statement would look like this:

```
SELECT * FROM Users WHERE UserId = 105; DROP TABLE Students;
```

Exercise 3:

IPSec protocol uses two protocols and two operating modes. Complete the following table that describes the components of an IP packet in each case where **{...}**: Authenticated. **[...]** : Encrypted.

Protocols	Modes	
	Transport	**Tunnel**
AH	**{**IP Header - AH Header - Data**}**.	**{**New IP Header - AH Header- original IP header – Data**}**.
ESP	**{**IP Header - ESP Header- **[**Data- ESP trailer**]** – Authentication Data**}**.	**{**New IP Header - ESP Header- **[**original IP header – Data- ESP trailer**]** – Authentication Data**}**.

Exercise 4:

Give a brief explanation of the following attack: ARP Poisoning, Smurf DDos Attack, Stack buffer overflow.

ARP Poisoning

An attacker making an ARP cache poisoning attack tries to inject false information into local area network traffic to redirect connections to their device. If the attacker succeeds, future connections to a specific IP address will be made to an attacker-controlled device because the connection initiator will find this false information in the cache and use it to establish its connection.

Smurf DDos Attack

The attacker sends ICMP requests (ICMP_Request) to broadcast machines with the victim's source IP address in the requests. Upon receiving ICMP requests all machines will send ICMP_Replay response packets to the victim's IP address. The target machine (victim) will find itself flooded with responses which will cause saturation and collapse of the system.

Stack buffer overflow

A stack is a region of memory that manages function execution in a program, storing local variables, return addresses, and other information. Stack buffer overflow occurs when a program writes more data to a local variable on the stack than it can hold, leading to an overwrite of return address. A hacker can Inject a malicious code or Jump to a malicious code