Assignment 1: Cryptography

**Federation University Australia at IIBIT (Sydney)**

**Sydney Campus**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ITECH** | **3** | **2** | **1** | **5** |

**COURSE NUMBER :**

**STUDENT’S GIVEN NAMES: KANCHAN SHRESTHA**

**STUDENT NUMBER FED UNI: 30344274**

**COURSE NAME: INFORMATION SECURITY**

**PROGRAM OF STUDY: Bachelor of Information Technology**

**TUTOR: ADNAN SAEED**

**TITLE OF ASSIGNMENT: CRYPTOGRAPHY**

**DUE DATE: 17 MARCH DATE SUBMITTED: 18 MARCH**

**DECLARATION:**

I have kept a copy of this assignment/work so that I can produce it if the original is lost or damaged. I hereby certify that no part of this assignment/work has been copied from any other student’s present or previous, published or unpublished, professional or amateur work or from any other source except where due acknowledgement is made in the assignment. I further certify that no part of this assignment/work has been written/produced for me by any other person except where such collaboration has been authorized by the unit/subject lecturer/tutor concerned.

----------------------------------------------------------------

Signature of Student

**Note**: It is necessary to sign the above declaration. A lecturer/tutor or an examiner reserves the right not to mark this assignment/work if the declaration has not been duly signed.

**Q1.**

1. **Name of the threat**

Distributed Denial-of-service attack

A Distributed Denial-of-service attack is a large scale DoS attack that interrupt normal traffic of a targeted server, service or network in great amount to the target or surrounding environment with a flood of internet traffic.

1. **System if attacks**

DDoS are designed to degrade online services like website, email and DNS services It attacks the host connected to the internet by flooding with the requests in attempting to overloading the system or the server and stopping other regular traffic from fulfilling their request or making the server unavailable for other users.

The system it attacks or the target system are: sites or services hosted on high-profile web servers like Banks, Credit card payment gateways.

Different DDoS attack vectors target varying components of a network connection. It attacks application layer (layer 7 of the OSI internet model), protocol attacks(layer 3 and 4 of the OSI model), also may exploit into the TCP handshake by sending large number of TCP requests. It may also attack multiple layer at the same time: targeting layer ¾ together with HTTP flooding that is layer 7. (Learning DDoS, 2019)

1. **How it perform it attacks?**

A DDoS attack requires an attacker to gain access of a network of online machines to carry out an attack. Uses multiple unique IP addresses or internet connected machines that are infected with malware that turns the devices into bots or zombies then attacker has remote control over the bots that turns them into botnet . It involves 3 to 5 nodes on different networks. When the connection between attacker and the botnet is established remotely, attacker sends updated instructions to each bot. Then the IP address of the victim is targeted by botnet and each bot respond by sending requests to the target causing the overflow of the server or network to overflow capacity causing Denial-of-service to the normal traffic. Since the fact that each bot is a legitimate internet device, it will be difficult to distinguish the attack traffic from the normal traffic.Depending upon the counter measure taken by the target, attacker may use one or multiple attack. That are

|  |  |
| --- | --- |
| Application Layer Attacks | It is a layer 7 DDoS attack where the webpages are generated on server and delivered in response to HTTP requests |
| Protocol Attacks | It is caused by consuming all the available table capacity of the web application servers and the available resources. It targets the vulnerables in layer 3 and 4 and cause service disturbance |
| Volumetric attacks | Attempting to create a traffic by using the bandwidths available between the target and internet and sending eh large amount of data creating huge requests from botnet by amplification |

1. **Mitigation Strategies**

Although organisations cannot fully avoid themselves from being targeted by the DDoS attacks, some of the countermeasures that the organisation can implement to reduce the impact are:

Identifying the Attack: Identifying the attack is the first step for mitigating the attack, some bot may be crawling the site that can reduce the availability of the website which is not actually a DDoS attack, Checking log data for checking if IP address are making high volume of requests in very short time and set up alerts to flag unusual from the normal traffic and block everything that appears to be suspicious (Matt, 2019)

Protect DNS servers: Protecting the servers by spreading servers across multiple data centres such as making data centres at different countries or different regions across same countries and check if there is no existing networks bottlenecks or failure of the network, distributing the servers geographically and topographically making the attackers difficult to attack more than one part of the server And leaving other servers unaffected by handling the normal traffic by the other parts

Some large site like Oracle Dyn has a deep internet infrastructure and security domain and a team of professionals to offer DDoS protection every minute with a managed support and contacts incase of the emergency. (Types of DDoS attack, n.d.)

1. **Scope of the threat**

Both cyber criminals and state nations could be exploiting this vulnerability. There are two common DoS attack they are Crashing the service and flooding the service. Individuals who are intending to hijack the online systems or the organisations from national level that are trying to shut down the online service that they don’t want can be the reason for DDoS attacks Some examples are: In 1996 Panix (third Oldest ISP- Inernet service provider in the world) was noted to be first attacked with SYN flood. In 2018, GitHub was attacked of 1.35 terabits per second. In October 2016 Mirai botnet attacked Dyn ISP that has sites such as Twitter, Netflix etc that made the website unreachable for hours causing costly for such large scale internet companies. (Bryan, n.d.)

1. **Concluding reflection**

In the world of Internet today, it has become quite common for hackers and attackers to conduct the cyberattack and DDoS is one of the key used attack in the large server to block the service of the sites by making information unavailable to the user and even causing a huge loss to the company. DDoS attack uses multiple system or compromised computer system as the attacking source like IoT devices or other network resources performing like a blockade in the highway of the regular traffic by preventing the regular flow of the traffic to the destination. Although it is not possible to avoid the attack countermeasures like limiting configuring the inbound and outbound network to limit unauthorised access and securing the configuration of available services at the application level to limit the risk.

**Q2.**

a.

|  |  |  |  |
| --- | --- | --- | --- |
| KEY | Key Size | Key Generation Time | Key ID |
| 1 | 1024 bits | 0.1 second | E3F2CC4B |
| 2 | 2000 bits | 0.5 second | DB880A29 |
| 3 | 3000 bits | 2 minutes | D8E3F866 |
| 4 | 3500 bits | 10 minutes | 226C74CC |

Key 1 was generated with the size of 1024 bits which is the least size for key generation and it took less than a mili second to generate the key. As the key was created of the small size it took comparatively least amount of time to generate the key. The second key took almost double the time as to the first key to generate. The size of the second key was as double the size of the first key. Not much variation in generation of the key so I decided to increase the size of the key and try it for 3000 bits. The variation I made was I changed the email address. I thought it took long time to generate the key for the 3000 bits size so according to the instruction I generated some variation in the input to generate random bytes by playing around mouse and keyboard that gives random number to gain enough entropy to generate the key.

A screenshot of a social media post

Description automatically generated A screenshot of text

Description automatically generated

Figure: Generating key with 4 different sizes for the RSA encryption scheme

b.

|  |  |
| --- | --- |
| **commands** | **action** |
| gpg –list-secret keys | Show list of secret keys |
| gpg –armora --export you@example.com > mykey.asc | Export the public key so that other people can have the key |
| “hexdump -Cv *filename*” | This command is used to display specified or inputs in a human related specified format |

A screenshot of a social media post

Description automatically generated

Figure : This is the encrypted message using one key

A picture containing table, computer, large, white

Description automatically generated

Figure: This is the portion of the encrypted data using hexdump -Cv “textfile” command

c. It took a long time to encrypt the 1GB file as the size of the file was so big that the enire process took almost an hour long to be encrypted and then decrypted. If the size of the file was less then it would take small amount of time.

A screenshot of a computer screen

Description automatically generated

d. The exported key is in an ASCII format because :  
The exported public key will be exported in a binary format which will be inconvenient while sending through emails and web that’s why GPG support command line option –armor that causes output to be generated in an ASCII-armored format which is like uuencoded document, the encrypted documents, keys and signatures by adding –armor option. (Trip Advisor, 2019)

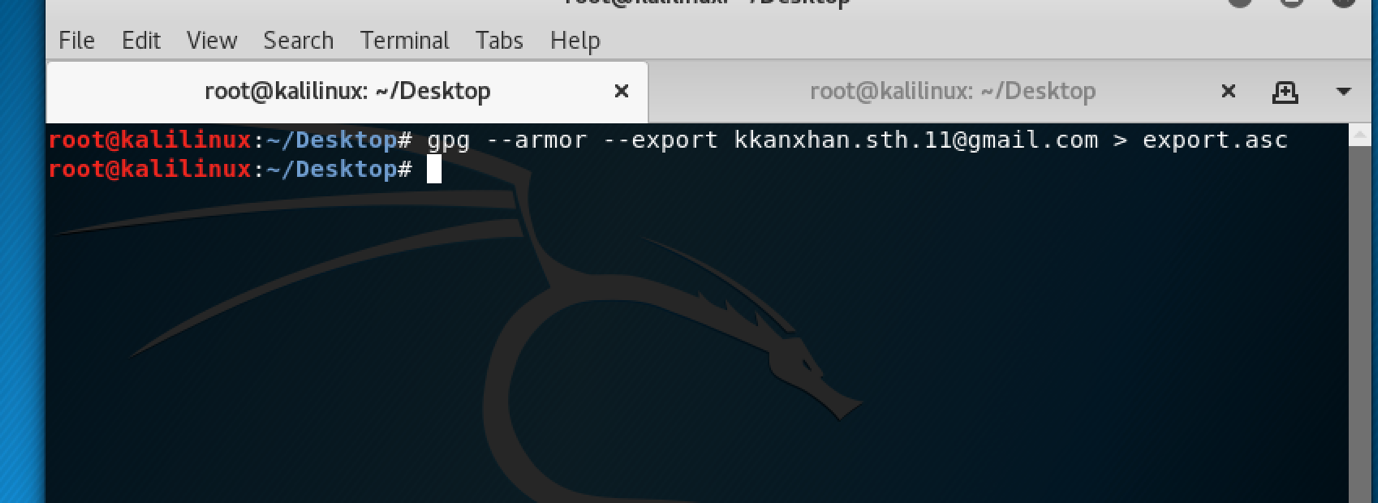




Figure. The exported public key in ASCII format

e.

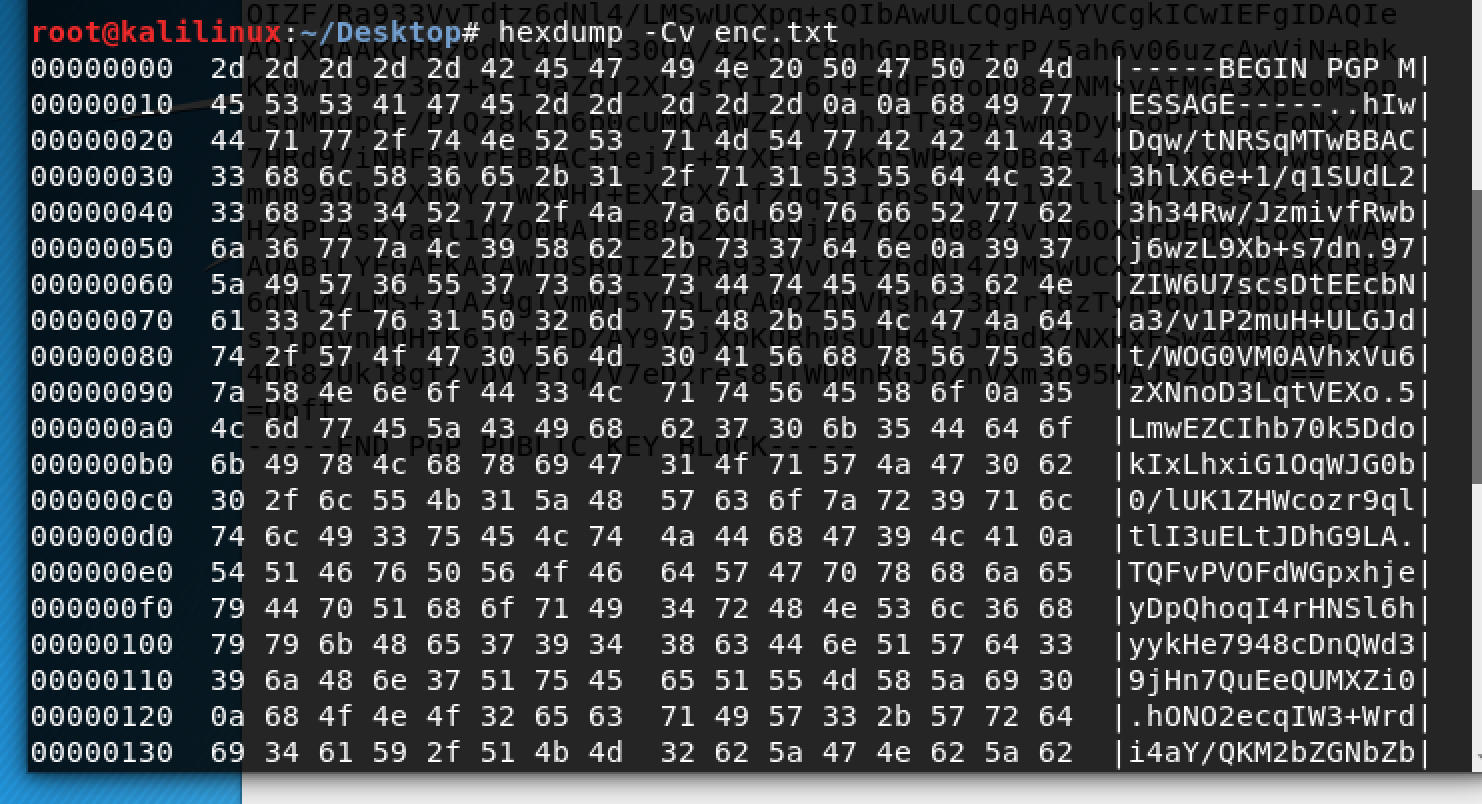


Figure: Encrypted a file containing ASCII text and display the cyphertext using the “hexdump -Cv *filename*” command

F.

G. **Role cryptography is playing in ensuring individual privacy in banking websites.**

Banks are one of the most important area where cryptography acts as the backbone of security.The banks have to go intuitively more and invest on data and information security due to the continuous surge in usage of online and mobile channels and the risk of various threats trigger the demand of Managing the security in online banking and phone banking which is being the most overwhelming challenge than compared to other transaction services. Cryptosystem or in the other word cryptography is the process of hiding the information by encrypting and decrypting the data through the use of a key. It works by encrypting that is converting plain text into unreadable or cipher text and decrypting which is bringing the unreadable text into its normal form by the use of secret key.

ATM also known as automated tailored machine which provides 24x7 service to the customer has made it easy to withdraw cash at given location providing cost effective banking. This is made possible because various encryption algorithms are build into the network to prevent the unauthorized transactions. Some examples of encryptions used in the mobile banking are OTP (One Time Password) which uses 4 digit encrypted pin while logging into the mobile online banking system. The OTP combined with SMS provides end to end secure connection and prevents unauthorised access. The OTP is generated using Powerful AES algorithm which uses 128 bits as a block for encryption using the encryption key it provides secure way of communicating in the bankings. Hence Cryptography plays and immense role in maintaining secure connections in banking website. (IOSR Journal of Business and Management (IOSR-JBM) , 2019)

# Bibliography

1. Bryan. (n.d.). *Responding to DDoS Attack*. Retrieved from Cyber: https://www.cyber.gov.au/publications/preparing-for-and-responding-to-denial-of-service-attacks
2. IOSR Journal of Business and Management (IOSR-JBM) . (2019). (pp. 33-37). IOS Journals.
3. *Learning DDoS*. (2019). Retrieved from Cloudfare: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
4. Matt. (2019). *Mitigation strategies for DDoS*. Retrieved from DYN: https://dyn.com/blog/six-steps-to-ddos-attack-mitigation-success/
5. *Trip Advisor*. (2019). Retrieved from https://mirrors.tripadvisor.com/centos-vault/3.7/docs/html/rhel-sbs-en-3/s1-gnupg-export.html
6. *Types of DDoS attack*. (n.d.). Retrieved from ECCouncil: https://blog.eccouncil.org/types-of-ddos-attacks-and-their-prevention-and-mitigation-strategy/