Department of Electrical and Computer Engineering

Florida International University

EEE 4717

Introduction to Security of Internet of Things

Project 3

1. (5 pts) Encrypt the message MIAMIBEACH using the RSA system with p = 43, q = 59 and e = 13, translating each letter into an integer (i.e., A corresponds to 00, B corresponds to 01, etc.)

MI=1208

AM=0012

IB=0801

EA=0400

CH= 0207

n=pq=43\*59=2537

cipher = (msg)emodN

(1208)13mod(2537)=0914

(0012)13mod(2537)=2497

(0801)13mod(2537)=0868

(0400)13mod(2537)=2210

(0207)13mod(2537)=1134

0914 2497 0868 2210 1134

2. (10 pts) Hands-On Exercise OpenSSL

OpenSSL is the most widely used open source cryptographic toolkit on UNIX- based systems. You can find it in the Kali Linux. It includes both a C library and a command line utility. In this hands-on exercise you are to experiment with the OpenSSL command line utility. First, answer the following questions and save your answers in a text file:

(a) Why are you taking this course?

(b) In which area(s) of security are you most interested in?

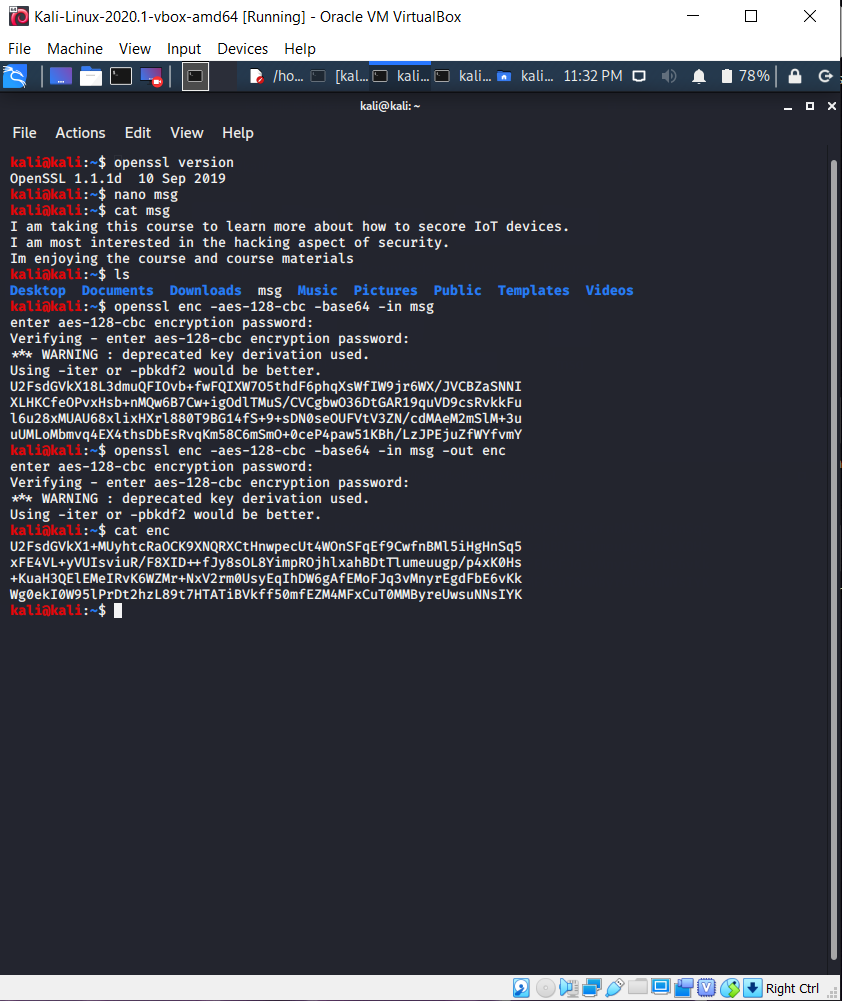
(c) What do you think about the course so far? Do you have any comments or expectations?

Encrypt your file using 128-bit AES in the CBC mode by running the openssl command. If your command is in the correct format, the OpenSSL command line utility will prompt you to enter a password, from which the key is derived. Use your FIU PID as your password. To test whether your encryption works, try decrypting your file after encryption. The webpage http://www.openssl.org/docs/apps/enc.html documents how to use openssl command to encrypt files, and you will find several examples at the bottom of this webpage. Ignore the command line option -salt shown in those examples on the webpage. To see list of all cipher names supported by openssl, run the following command: openssl help.

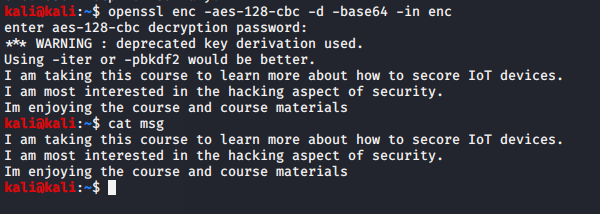
Name the ciphertext file: yourPID.enc.

File attached named 5734454.enc

Encrypting process:



Decrypted:



3. (15 pts) Hands-On Exercise GPG

GNU Privacy Guard (GnuPG or GPG) is a free software replacement for Pretty Good Privacy (PGP), a popular software application that provides the ability to encrypt and digitally sign files and email messages. GPG is interoperable with current versions of PGP. Kali Linux has the Linux version of GPG. You can either use the Linux version or the Windows version of GPG for this assignment. The Microsoft Windows version of GPG can be downloaded from <http://www.gpg4win.org>.

GPG is a hybrid cryptosystem. In other words, a file is encrypted with a random session key using symmetric key techniques (such as AES). The session key is encrypted with the intended recipients public key and attached to the encrypted file. The recipient uses her/his private key to recover the session key, which is then used to decrypt the file. A file is digitally signed with the signer’s private key and verified with the signer’s public key.

Each GPG user maintains a keyring, which is a database of other people’s public keys that the user trusts. Each user decides by oneself which key to trust. Instead of relying on any certificate authority, GPG uses the web of trust model for public key management. That is, any user can sign another user’s public key, thus vouching for that public key. If you trust that voucher, you may also trust that public key and import it to your keyring. There are several ways to distribute your public key. You may publish it on a PGP/GPG key server so that other people can download it. You may also save it as an ASCIIarmored file and send it to your friends.

(a) Generating your public-private key pair (Windows version, for the Linux version please study the Linux manual using the command “man gpg” )

i. Run the program and open Key Manager. Choose Generate a GnuPG key pair and click OK. Follow the Key Generation Wizard to create your public-private key pair. When the wizard completes, you will see your key pair listed in your keyring. Your key should be a RSA/2048 key that never expires. If you wish to publish your public key on a key server, you may rightclick your key pair in your keyring, click Publish on Server.

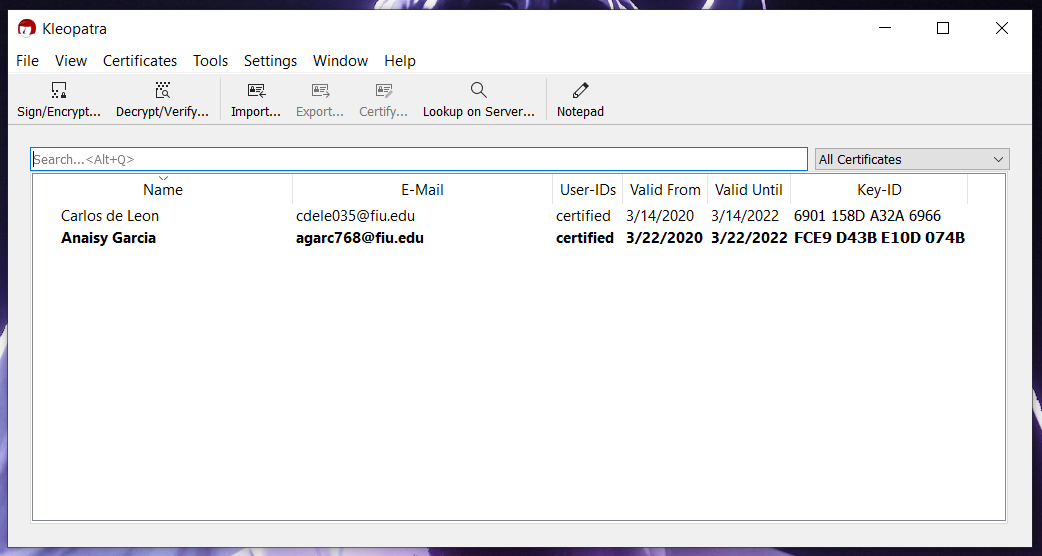
ii. You will see your GPG fingerprint, which is a hash of your public key at the bottom of the window. Write it down. It can be used by other people to authenticate your public key. GPG users often publish their GPG fingerprints on their websites or print them on their business cards, so that you may check whether a public key that you have obtained is indeed your friends key by comparing its fingerprint with the fingerprint published on your friends homepage, for example.

iii. Highlight your key pair and choose Export from the Key menu to save your public key as an ASCII armored file, which has an .asc extension.

iv. Send the ASCII-armored file to one of your peers in class (you can use the Project 3 Forum for finding your peer and upload your public key file) and ask your peer to sign your public key. To sign the public key of someone else, you must import it to your keyring first following the instructions to import that public key. Then right-click that public key in your keyring and click Sign. When it is done, goto Preferences under Edit and check the Use advance mode box. You will find Signatures and Subkeys tab listed at the bottom of Key Manager where you can check your signature. Now export it to an ASCII-armored file and send it back to the owner.

v. Your signed public key file “filename.asc" must be submitted for grading. Make sure that you are sending a signed public key file, not your original public key file. Also put down your GPG fingerprint in a text file named GPGXXX.txt where XXX is yourname and submit it as well.

First file is called Key.asc.gpg and the second file is GPGAnaisyGarcia.txt.



(b) Encrypting and signing a file

i) Go to http://keys.gnupg.net. Enter your Instructor name in the text box and click Search to search for your Instructor public key. The search engine may list multiple public keys that all seem like your Instructor public key, however only one of them is valid. Determine which one is valid using your Instructor GPG fingerprint posted in the course and import it to your keyring using keyid.

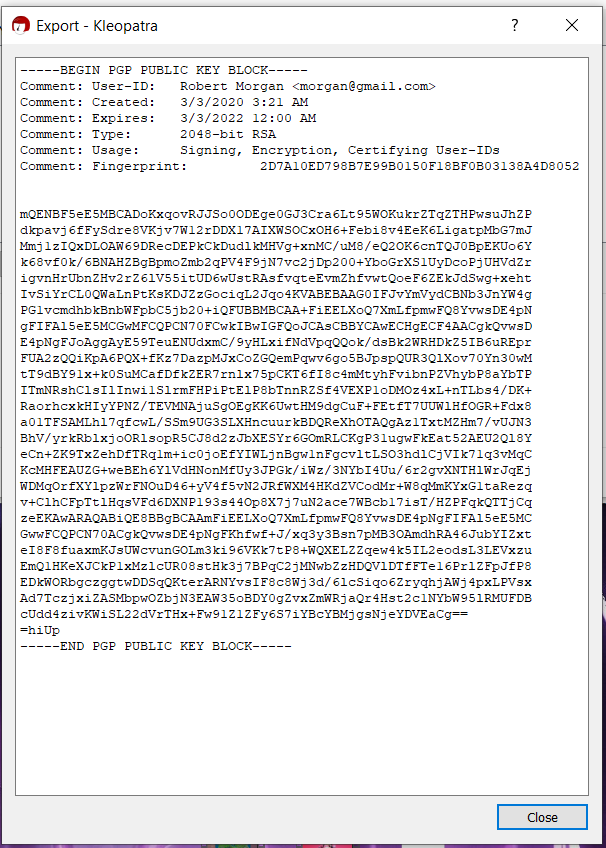
ii) Write down the algorithm, size, date of creation and expiry date of her public key.

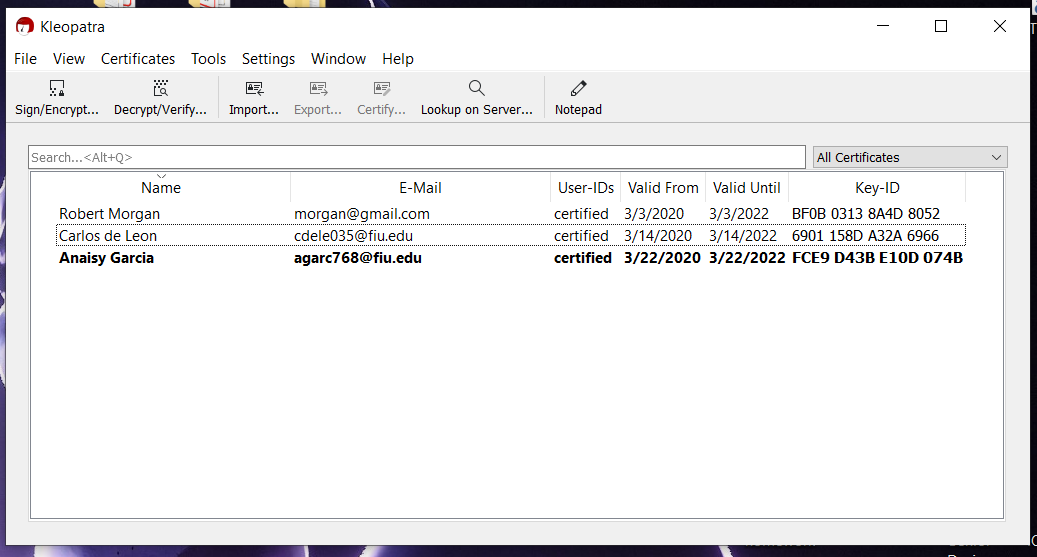
iii) Create a text file named p3.txt. Put down your name as well as the aforementioned information about your instructor’s public key in this file. Moreover, write a paragraph telling us how you think about GPG. For example, do you think GPG is user-friendly? How do you think about the web of trust model? Any feedback regarding the course and the assignments is also welcomed. For example, are the hands-on exercises interesting or are they too tough?

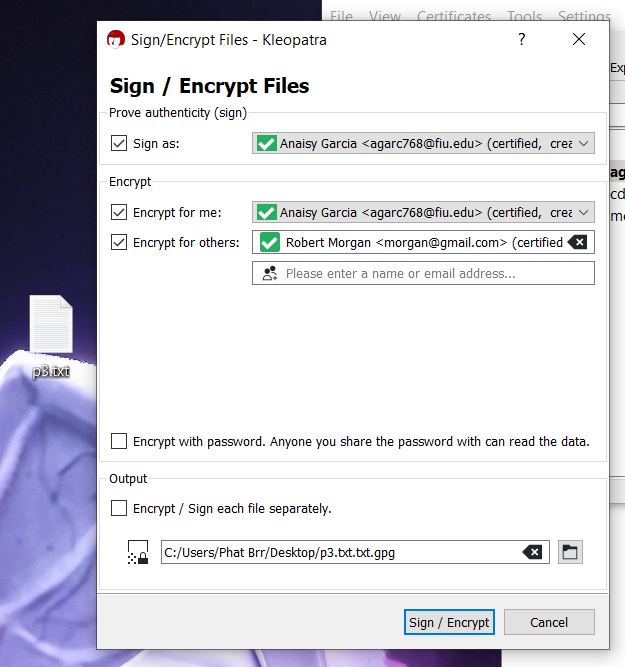
iv) Browse for p3.txt under Windows. Select your instructor’s public key for encrypting and your own private key for digitally signing p3.txt. Check the box that reads Text output (ASCII Armor).

v) Submit the encrypted-and-signed file p3.txt.asc.

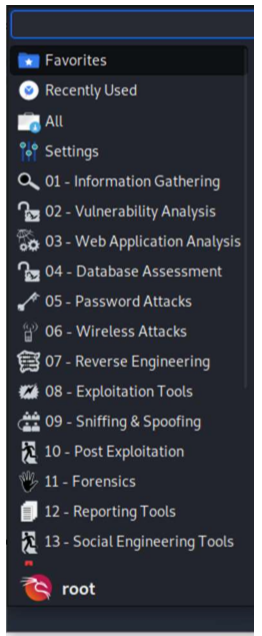
Submitted File is called p3.txt.asc.







4. (25 pts) Kali Linux has many tools that you can used for various purposes. See the figure below.



Select 5 tools (from any category) that you think the most useful tool. Explain your reason. Also provide a brief description for each of your chosen tool.

01 – Information Gathering – MOST USEFUL

This is the most useful due to them being mostly free and helpful for the passive reconnaissance phase of hacking. The tools under this category are used to gather information about an individual, a company, or a device among others.

05 – Password Attacks –

These types of tools are used for penetration testing. These can help people working in IT fields access and test security of the systems they are testing. This then allows them to maintain and update the security of these systems.

06- Wireless Attacks –

These types of tools are used for cracking and hacking wireless networks. These tools allow for checking the security of a wireless security system and allows for gathering information of any device connected to a wireless network.

09- Sniffing & Spoofing-

These types of tools are used to check the security of web security. These are more commonly used for network capture analysis.

12- Reporting Tools –

These types of tools allow for tracking, sharing, and documenting, hacking or testing results. These tools can also be used to download documents onto a computers local disk directly from the internet.

5. (45 pts) Lab Cisco – Threat Identification (see another pdf file)

Lab – Threat Identification

Objectives

Explore the security features used by organizations to keep data safe.

Part 1: Exploring the Threat of Cyberattacks

Part 2: CIA Triad

Background / Scenario

The threats posed by the cyber world are real. These threats have the potential to wreak havoc on life in a computer centric world. Understanding these threats is important to everyone and in order to combat them, the world needs committed individuals that can recognize threats, and outmaneuver and outsmart cyber criminals. In order to develop the talent needed, organizations like CompTIA, Cisco Systems and ISC2 have created programs to educate and certify cyber professionals.

Required Resources

• PC or mobile device with Internet access

Part 1: Exploring the Threat of Cyberattacks

Cyberattacks top the list of threats facing countries around the world. When people think of threats to national or world security, most people think of physical attacks or weapons of mass destruction. The fact is cyber threats top the list in over twenty countries around the world. The ranking of cyberattacks in the number one spot reveals a few things about how society has changed. Computers and computer networks affect the way we learn, shop, communicate, travel, and live. Computer systems control almost every aspect of our lives. The disruption of computer systems and computer networks can have a devastating impact on modern life. Electrical power generation and distribution systems, water treatment and supply systems, transportation, and financial systems are all targets of cyberattacks. Each of these systems has been a victim of cyberattacks. Watch the video below. Break into groups of 3-4 people. After viewing the video, answer the questions below.

Step 1: Research Threats.

In step 1, you will research threats.

1. Click here to view the video. According to the video, what is the most dangerous weapon in the world? Why? Do you agree?
   * 1. According to the video, the most dangerous weapon in the world is a computer because in the hands of a criminal can erase your identity, bring down wall street, ground airplanes, take out the power grid, and wreak havoc on our entire economy. I agree that a computer is a very powerful weapon if connected to a network. I personally believe without network access cybercriminals cannot do what they do. A gun cannot do any damage without a bullet. A computer alone isn’t enough to commit cybercrimes. The computer is a weapon, but the internet is the bullet.
2. List five ways a cyber-criminal can use computers to break the law. Can any of the crimes you listed affect you personally? Have you or your family members been affected by these crimes?
   * 1. The first is hacking. This is an act committed by an intruder by accessing a computer system without the computer owner’s permission. The second is the act of installing a virus on a victim’s computer. This can disrupt the computer operation and affect the data stored on it either by modifying or deleting it. The third is a logic bomb. A logic bomb is a piece of malicious code that is installed in software on purpose to execute a malicious task when triggered by a specific event. The fourth is a DoS attack. This is the act of flooding a computer with multiple resource requests that can cause a server overload. This can cause a web server, for example, to crash and slow down. The fifth is phishing. This is a technique of extracting confidential information such as credit card numbers or passwords by disguising themselves as a legitimate corporation.
3. Have any of the potential threats portrayed in the video actually happened? Click here to learn more about these attacks.
   * 1. All the above crimes can affect me due to me using the internet. I download a lot of games online and any of those could eventually bite me back. Many of my family members have been victims of viruses. Since viruses are everywhere and they’re so easy to fool someone with I see why. My grandfather always plays online poker and that is usually where they get him from. My father has had his identity stolen twice in the past two to three years.

Step 2: Explore Recent Attacks.

1. The impact and scope of recent cyberattacks have many business and government officials concerned. Click here to review the top 10 most devastating cyber hacks or 2015. How many people did the US Office of Personnel Management data breach affect?
   * 1. This breach is a data theft consisted of stealing addresses, health information, and financial details of 19.7 million people who were subjected to government background checks, as well as 1.8 million others.
2. Describe the TalkTalk attack of 2015. Who was responsible and what did the cyber criminals steal?
   * 1. The mobile phone provider was the target of a group of teenage hackers who stole the customer information details of over twenty thousand customers.

Part 2: CIA Triad

Confidentiality, integrity, and availability are the three fundamental cybersecurity principles. These three principles make up the CIA triad. The elements of the triad are the three most crucial components of security. All cybersecurity professionals should be familiar with these core principles.

Step 1: Explore the CIA Triad.

1. Click here to view the video. What is data confidentiality? Why is data confidentiality so important to people and organizations?
   * 1. Confidentiality is protecting the privacy of information. People and companies use information systems for many activities. When using computer systems, people and companies are required to share very sensitive data. The other companies that collect this data are responsible for its security and concealment. In the hands of a threat attacker, sensitive information can be misused to commit crimes.
2. What is data integrity? Name three ways data integrity or trustworthiness is affected.
   * 1. Data integrity is the principle of protecting and maintaining the consistency, accuracy, and trustworthiness of data. Equipment failure, errors, human mistakes, or attacks by a threat actor who intentionally change, delete or damage data, are examples of how data integrity is affected.
3. What is system availability? What can happen if a critical computer system is no longer available?
   * 1. The cybersecurity of availability states that information and information systems must be obtainable when required. System availability must have correctly operative computing systems, services and communication channels. Loss of availability can affect services and access to data on the systems. For example, a bank system availability failure. Here a bank customer would not be able to deposit or withdraw money to or from the bank.

Step 2: Explore Cyberattacks.

Click here to watch a video. What were the cybercriminals trying to do? What time of the day did the attack occur? Are network attacks likely to occur after hours? Why?

The threat actors were attempting to gain access to the Garrison Inc. network. The attack took place at 17:00 on a Friday. Most external network attacks will occur after work hours because the company is less likely to find the attack.