ISEC 325 Homework 04

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [3 points] List and briefly describe the three basic operations involved in encryption. Explain why repeated use of the /same/ operation is no stronger than just using it once (give an example), but yet combining two or more different methods is extremely powerful.

   The three basic operations involved in encryption are substitution, transposition and XOR. A substitution cypher is where one value is substituted for another. Transposition is when one letter becomes another letter and a key must be used to decrypt. Transposition is rearranging the message putting the letters out of order. In transposition a matrix is used to place the words left to right top to bottom. The letters are then laid out in vertical rows to create the scrambled text. XOR is binary math where you convert your message to bits you then create a key which is the second bit. The two are added up which gives you the result and the encrypted message. Using the same method twice doesn't benefit you because the same process can be used to decrypt the message it just may take a bit longer. If you use two different types, it makes it substantially more difficult because you would need to know the substitution for example and possess the key from transpositions matrix or the key from XORs binary conversion.

2. [2 points] What is a hash function and what is it used for?

   A hash function is a mathematical algorithm that creates a message summary or digest that can be used to confirm the identity of a specific message or confirm that the message has not been altered. They are one-way algorithms that are difficult to reverse. If hashing is used for passwords in a database, the hash is applied to the password and the result is stored in the database. The next time the user logs in the same process is done and the hashes are compared if they match the password is correct.

3. [3 points] What is the fundamental difference between symmetric and asymmetric encryption?

   Symmetric encryption uses a single key to both encrypt and decrypt a message. The key in symmetrical must be sent out of band that is not with the message but with a different means, so it does not get intercepted. Asymmetrical encryption uses two different but related keys and either can be used to encrypt or decrypt the message. If key one is used to encrypt a message in asymmetrical then key two must decrypt and if key two is used to encrypt then only key one can decrypt.

4. [2 points] How does the Public Key Infrastructure (PKI) protect information?

   PKI is an integrated system of software that uses digital certificates and certificate authorities to protect information. Digital certificates are public key container files that allow computer programs to validate keys and identify who they belong to. Certificate authorities keep the digital certificates. If someone wants to send an encrypted message, they obtain the digital certificate which is validated by the certificate authority and encrypts to the recipient who then can use their private key to decrypt.

5. [2 points] Why is the size of a key important in cryptography?

Key size is important in cryptography because the strength of applications and cryptosystems is determined by key size. The longer the key size the stronger the encryption will be.

6. [5 points] Describe, in your own words, the mechanism for establishing a HTTPS connection.
You request connection with a website through your application. The website sends you the websites security certificate back. You then use the public key in the certificate to encrypt a random secret key generated by your application or browser which is sent back to the website for symmetrical encryption. You then use the random key generated for the rest of the conversation.

7. [8 points] The following cyphertext uses a substitution cypher. Decrypt the original message and show the key that you used. Doing this by hand may take a while, but consider character frequencies to start and then other hints (such as double letters and short words like “the” “are” and “and”).

OJGFIVUZ NVJ GTJ HNDIV PIKOG IW JOGVM GI HIZG CIHPSGJV ZMZGJHZ. PVJLJOGKOA SOFNOGJQ KOGVSZKIO, SZJ, NESZJ, IV WYIIQKOA IW CIHHSOKCNGKIOZ CTNOOJYZ KZ N TKAT PVKIVKGM GI IVANOKXNGKIOZ GVMKOA GI PVIGJCG GTJKV NZZJGZ. OJGFIVU ZJCSVKGM KZ NEISG PVJZJVLKOA GTJ NPPVIPVKNGJ SZJ IW OJGFIVU VJZISVCJZ FTKYJ PVJLJOGKOA QKZNYYIFJQ SZJ. KO GTKZ CISVZJ, MIS FKYY YJNVO TIF GI JHPYIM WKVJFNYYZ, LPOZ, NOQ ZGNGJWSY PNCUJG KOZPJCGKIO GJCTOKBSJZ GI TNVQJO CIHPSGJV OJGFIVUZ. GIPKCZ KOCYSQJ PNCUJG WKYGJVKOA, KOGVSZKIO QJGJCGKIO NOQ PVJLJOGKIO, KOAVJZZ NOQ JAVJZZ VSYJZ, HIOKGIVKOA, OJGFIVU NCCJZZ CIOGVIYZ, NSGTJOGKCNGKIO, NSGTIVKXNGKIO, NOQ NSQKGKOA.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

GQCJBWTMOEIVYANPDXUHKRFZLS-Key used

Networks are the major point of entry to most computer systems. Preventing unwanted intrusion use abuse or flooding of communications channels is a high priority to organizations trying to protect their assets. Network security is about preserving the appropriate use of network resources while preventing disallowed use. In this course you will learn how to employ firewalls vpns and stateful packet inspection techniques to harden computer networks. Topics include packet filtering, intrusion detection and prevention, ingress and egress rules, monitoring network access controls, authentication, authorization and auditing.

8. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

I found this week's chapter to be a nice review/overview of cryptography to be very useful. Last semester I took WEBD236 and the instructor took extra time and went over hashes and salts with me in that class we also covered HTTPS in depth. I didn't really get encryption before that class. I did some extra reading on it on my own. Hashing is supposed to be a major part of security certificates. I wanted to know how hashing worked for the future.

I don't think before this week that I had a firm grasp of what the difference between asymmetrical and symmetrical encryption was. I had read about asymmetrical encryption in a programming class with examples set up with cans of paint. I have been teaching what I learn in class to my wife and a friend at work so when I come up not knowing exactly how to explain it, I know I don't fully understand.

I went to YouTube and watched a video explaining asymmetrical encryption with the paint examples and it made a lot of sense to me. I feel like I understand now the difference between the two and what goes on between the application and browser in https.

Encryption seems like it is very robust if it is handled properly. The means to try and break it seem like they can take a long time. It seems like the way people run into trouble is not having the time or resources to set up their security properly. I did not see anything in our homework or in the homework container about a WPA2/WEP video that we are supposed to watch or anything in the homework about that. You had mentioned a video in the MEET and something about a table we would have to refer to. I don't know if that is missing in the homework document or in the container.

References

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.