# 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. Substitution means that the one-bit pattern is taken and exchanged for another. Transposition is taking the existing bits and moving them within their block or stream. XOR means that the bits are taken and XORed with some elements of a key. Using one operation multiple times is not stronger as it does not make much of a difference as if it was run once. The substitution takes a pattern and exchanges it for another which means the whole pattern is exchanged. Doing this multiple times will just land with a single pattern and now real show of change as it would if it was directly exchanged to the new pattern. Looking at it, a person may not be able to tell that it went through multiple changes because a single change would end up in the same place. Combining two or more does make a significant difference as they interact with different levels of the encryption. The substitution is used to take a complete bit pattern and change it with another while the transposition will change up the bits in the block to help shuffle it more. The XOR will interact with the bits themselves so by XORing the bits them shuffling them, followed by changing the pattern, it will lead to better encryption.

1. [2 points] What is a hash function and what is it used for?

The hash function is a message summary which tells the person if the message contents have been changed. This helps a person determine if there are more steps, they need to follow to get the encrypted message.

1. [3 points] What is the fundamental difference between symmetric and asymmetric encryption?

The fundamental difference between symmetric and asymmetric encryption is how a key is used to encipher or decipher a message. The symmetric encryption means that the same key that was used to encipher the message can be used as well to decipher the message. The asymmetric encryption means that the message will need to different keys as one can encipher but the other is needed to decipher the message.

1. [2 points] How does the Public Key Infrastructure (PKI) protect information?

The PKI protects information by providing digital certificates and encrypting any data that it plans to send between parties while providing each with a key that can be used to encrypt or decrypt the information. PKI focuses on making sure that information is secure while it is being sent between parties and uses certificates to make sure that the information is being sent to the right parties.

1. [2 points] Why is the size of a key important in cryptography?

The key is used to provide a level of security and the size will directly affect the security of it. Say a key is set up to show that the message has the letters a and o switched, this would provide a tiny bit of security as it would take time to switch back the letters but would not be hard to figure out. If each letter of the alphabet and each number was randomly switched with another, then it would be more secure as it would take more time to try to break.

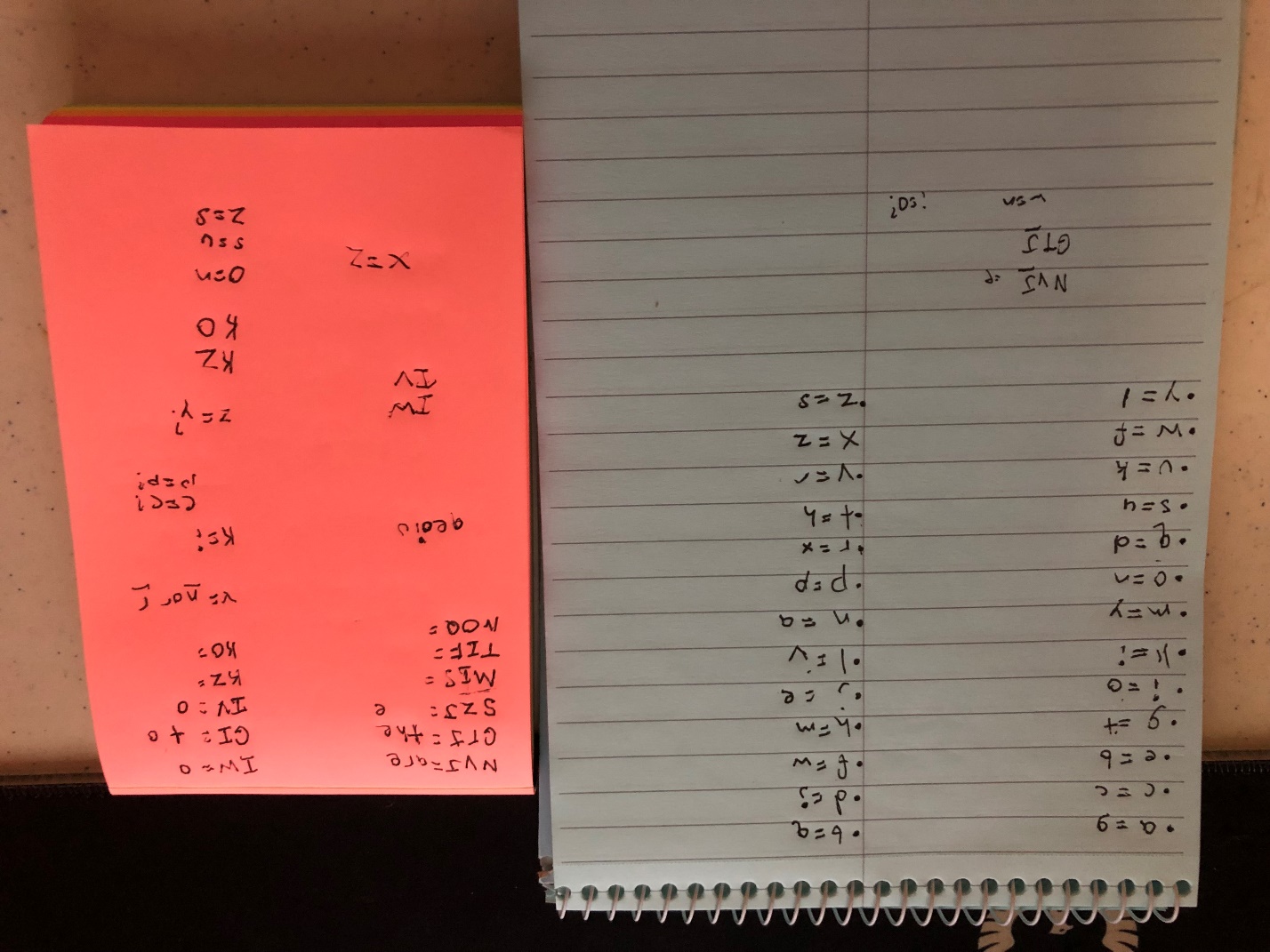
1. [5 points] Describe, in your own words, the mechanism for establishing a HTTPS connection.

Establishing a HTTPS connection starts but getting the site’s certificate and verifying that it is correct. Then the public key in the certificate is used for getting a randomly generated key created through the browser for the symmetric encryption. The new key is then sent to the server so it knows to send your messages to your indicated target and receive them back.

1. [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.

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.



1. [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.

This week we worked on cryptography and the parts that are used in encrypting and decrypting messages. Encryption is a topic that I really enjoy as it has different ciphers to use and keys for determining what the message is. The last homework problem was to take a cypher and decrypt it while then providing a key. I took a bit by taking the message and moving it to a word doc where I could highlight then entire thing and work to slowly change the text. I found it best to find the letters e, a and i first as these tend to appear a lot in text as e is part of many common three letter words like the and are while the other two letters can be part of three two or even be by themselves. It took a while to figure out, but I had a lot of fun with it, and it is a good message. Most encryptions can be in a way where a computer cam figure it out and solve it once handed the key, but I find it fun to be able to do it by hand and watch as the message forms. These are the types of activities that I would love to do more of and enjoy a lot.