C20483462 Jamie Heffernan

Advanced Security 01 – Assignment 01

1.

In today's day and age, every movement made in a web-browser is tracked and traced, this is generally for monetary gain but could also be for malicious reasons such as identity theft or fraud. For this reason, we want to limit the amount of information we expose online through the use of some cryptographic applications such as:

VPN

A Virtual Private Network or VPN encrypts your internet connection by creating an encrypted 'tunnel' between your device and the VPN server. This level of encryption protects your data from potential hackers who may try to intercept your data as it goes out on the network, with the use of a VPN any data that is captured will be useless without the VPN's decryption key thus adding a layer of protection when using unsecured networks

Tor Browser

The Onion Router or TOR is a web browser which uses a layered approach to encryption to enhance user security and privacy. When using Tor, your data is encrypted multiple times and routed through a series of servers called nodes. Each node peels back one layer of encryption to reveal the instructions for the next hop before passing the data to the next node. This process provides excellent privacy and anonymity online making it difficult for anyone to track the origin or destination of the data

HTTPS Everywhere

This is a browser extension to automatically encrypt your connection to websites by ensuring that the Secure version of the HTTP protocol (HTTPS) is used whenever and wherever possible, it does this by rewriting URLs from HTTP to HTTPS which encrypts all data exchanged between your web browser and a given website

Disconnect

Disconnect is a powerful browser extension which allows a user to gain insight into online tracking by providing a visual representation of trackers on a given website. Disconnect actively blocks many forms of tracking such as cookies, beacons and other data collection methods, this allows users to understand who is trying to track their activity online. Disconnect displays the types of trackers employed on a website and allows them to block individual or all trackers

In conclusion there are many methods of preventing malicious actors tracking you or gaining access to sensitive data when browsing the internet but by combining multiple encryption methods, you can exponentially increase your security and privacy on the internet. I would switch to Tor browser, while using a VPN and the HTTPS Everywhere and Disconnect extensions to maximize my privacy and security on the internet.

2.

See Assignment1.py

3.

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE

ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL

VARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND

JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO

THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE

TOP ROW AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW.

FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET,

BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS)

AND THEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR

THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE

THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU

WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE

THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.

4.

The key used to encrypt the text was 17.

We could try to brute force the encrypted message by trying every possible shift from 1-26 until we get a legible message however without the aid of a computer this would take a while. The first step to decrypt this code was to analyze the ciphertext, what can we learn from it without the decryption key? If we read through the ciphertext the string “SFKKFD” appears midway through the message, this encrypted string has 6 characters however we can see that only 4 of these are unique, and two of them are right next to each other, not many letters in the English language can be grouped together like that, mainly e,r,t,o,p,s,f,l,z,c,n and m. This one string of characters has brought the possible permutations of the encryption down from 26 to 12, less than half of the original. We can reduce this even further as the double letters in the middle are surrounded by the same letter each side meaning that the second and fifth characters are most likely a vowel, a, e, I, o, or u. This brings the number of possible combinations down even further, to 5 and with that we can begin brute forcing this string with either a computer or by aligning two pieces of paper with the alphabet written on them, and after some trial and error, the word BOTTOM reveals itself with a decryption key of -17.

5.

NIST IS ABOUT TO ANNOUNCE THE NEW HASH ALGORITHM THAT WILL BECOME SHA-3. THIS IS THE RESULT OF A SIX-YEAR COMPETITION, AND MY OWN SKEIN IS ONE OF THE FIVE REMAINING FINALISTS (OUT OF AN INITIAL 64). IT'S PROBABLY TOO LATE FOR ME TO AFFECT THE FINAL DECISION, BUT I AM HOPING FOR "NO AWARD." IT'S NOT THAT THE NEW HASH FUNCTIONS AREN'T ANY GOOD, IT'S THAT WE DON'T REALLY NEED ONE. WHEN WE STARTED THIS PROCESS BACK IN 2006, IT LOOKED AS IF WE WOULD BE NEEDING A NEW HASH FUNCTION SOON. THE SHA FAMILY (WHICH IS REALLY PART OF THE MD4 AND MD5 FAMILY), WAS UNDER INCREASING PRESSURE FROM NEW TYPES OF CRYPTANALYSIS. WE DIDN'T KNOW HOW LONG THE VARIOUS SHA-2 VARIANTS WOULD REMAIN SECURE. BUT IT'S 2012, AND SHA-512 IS STILL LOOKING GOOD.

6.

See Assignment1.py