

ENTS 689i: Network Immunity

Problem Set #1 Solutions

1. Chapter 2, Problem 2

Caesar cipher with a rotation of 21 characters

Plaintext: THERE ARE TWO THINGS TO AIM AT IN LIFE, FIRST TO GET WHAT YOU WANT AND AFTER THAT TO ENJOY IT. ONLY THE WISEST OF MANKIND ACHIEVE THE SECOND.

2. Chapter 2, Problem 10

Substitution cipher based on a simple pattern mapping plaintext to ciphertext.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	M	O	L	P	K	Q	J	R	I	S	H	T	G	U	F	V	E	W	D	X	C	Y	B	Z	A

Notice the ciphertext is the first half of the alphabet reversed, interleaved with the second half of the alphabet.

Plaintext: 'T WAS BRILLIG, AND THE SLITHY TOVES DID GYRE AND GIMBLE IN THE WABE: ALL MIMSY WERE THE BOROGROVES AND THE MOME RATHS OUT GRABE.

(Part of the Jabberwocky poem by Lewis Carroll, 1872)

3. Chapter 2, Problem 16

Perform a frequency analysis, and see if the distribution of characters is similar to a permuted distribution of the likely language of the plaintext. This can be accomplished by sorting the distributions of both the target language and the ciphertext and see if they are similar.

4. Chapter 2, Problem 17

Perform a frequency analysis, and see if the distribution of characters is similar to an unpermuted distribution of the likely language of the plaintext.

5. Chapter 2, Problem 22

See Table 2-3 from the textbook, on page 61. Stream ciphers are typically used when large volumes of streaming data needs to be encrypted with low latency (i.e. VPNs, L2 encryption, file encryption), and block ciphers are used when we're encrypting smaller blocks of data where latency is less of a concern (i.e. email). If looking at sheer volume of encrypted traffic, stream ciphers are more prevalent. AES-CCM is becoming popular as using a block cipher to create a stream cipher.

6. Chapter 10, Problem 21

Need $p \cdot q > 2^{12} = 4096$

$p=67$ and $q=71$ are a set of primes that work; there are others

7. Chapter 10, Problem 22

DES is a bijection, and is therefore an onto function. DES is a bijection because we need $P=D(E(P))$. If two ciphertexts mapped to the same plaintext, or vice versa, we wouldn't be able to uniquely encrypt and then decrypt a message. Since any plaintext is possible, any ciphertext must also be possible, since they are both 64 bits in length.