Chris Wozniak - 10109820
Introduction to Cryptography CPSC 418 Fall 2015
Department of Computer Science
University of Calgary

October 4, 2015

HOME WORK #1

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. Substitution

Compute the plaintext from the provided ciphertext. Code created for solution attached to assignment.

(a) Letter Frequency Analysis:

(X | 136)	(A | 46)	(S | 16)
(O | 85)	(F | 31)	(G | 14)
(J | 72)	(N | 31)	(V | 9)
(R | 59)	(K | 29)	(M | 8)
(P | 57)	(E | 27)	(H | 5)
(T | 57)	(Z | 24)	(B | 3)
(U | 57)	(D | 20)	(Y | 3)
(I | 56)	(L | 19)	(W | 2)
(C | 47)	(Q | 17)	

(b) Decrypted plaintext:

Case was twenty-four. At twenty-two he'd been a cowboy, a rustler, one of the best in the sprawl. He'd been trained by the best, by McCoy Pauley and Bobby Quine, legends in the biz. He'd operated on an almost permanent adrenaline high, a by-product of youth and proficiency. Jacked into a custom cyberspace deck hat, projected his disembodied consciousness into the consensual hallucination that was the matrix. A thief, he'd worked for other wealthier thieves. Employers who provided the exotic software required to penetrate the bright walls of corporate systems, opening windows into rich fields of data.

He'd made the classic mistake, the one he'd sworn he'd never make: he stole from his employers. He kept something for himself and tried to move it through a fence in amsterdam. He still wasn't sure how he'd been discovered, not that it mattered. Now he'd expected to die then but they only smiled, of course he was welcome. They told him welcome to the money and he was going to need it, because still smiling they were going to make sure he never worked again.

They damaged his nervous system with a wartime "Russian Mycotoxin"

(c) Who originally wrote the plaintext? (Bonus)

William Gibson, Neuromancer

⟶ Answer

Problem 2. Compound Cipher Theory

The shift cipher.

(a) Give a formal proof that multiple shifts results in a shift cipher.
   i. eK1 + ek2 = ek1+k2
   ii. multiple enumeration

(b) Multiple encryption
   i. Vigenere key pairs
   ii. Vigenere double encryption

$\longrightarrow$ Answer

Problem 3. Entropy

(a) Entropy
(b) Maximal
(c) Maximal Value of H(x)

$\longrightarrow$ Answer

Problem 4. Password lengths

(a) Total number of ASCII encodings

(b) Unusable ascii codes

   i. key space sizes

   ii. percentage of ascii codes are permissible

(c) Entropy of keyspace

(d) Entropy of restricted keyspace

(e) Entropy 128

   i. all ascii chars

   ii. ascii lower case restricted

⟶ Answer

Submitted by Chris Wozniak - 10109820 on October 4, 2015.