CS 458 Information Security

Homework 1: Administrivia, Historical Cryptography

1. Administrivia

(a) Are following activities encouraged (E) or forbidden (F)?

[Encouraged] Discussing course materials on piazza
[Encouraged] Discussing homework problems
[*see below] Sharing your homework solution with others
[Forbidden] Sharing quiz answers
[Forbidden] Looking at others' exam

* While normally sharing homework solution is a violation of academic integrity, this course has only ungraded homework, therefore, you're free to share and discuss your solutions with your classmates. However, we strongly recommend you to finish each homework independently before such discussion.

(b) Where can you find a copy of the textbook (and other resources) for free?

IIT Library

(c) [False] Going through slides will be enough review for exams.

(d) What "pain points" do you anticipate for this class? How should you prepare for them?

This introductory course will touch on a variety of subjects, some of which you might not have sufficient background in. Solution: Google a lot. Piazza a lot. Read a lot. Ask a lot. And while you're at it, help each other!

2. Key concepts

(a) The three most important components of computer security, known as the "CIA triad", are what?

Confidentiality, Integrity, Availability.

(b) Read the scenario, and identify each item as a threat, an asset, a vulnerability, an attack, a countermeasure, or an adversary.

Scenario: A hypothetical student broke into an office, installed a keylogger, intercepted login and password, and obtained the hypothetical final exam ahead of time. Department found out, replaced the hypothetical exam, and checked all computers for keyloggers.

Identify:

- (adversary) the hypothetical student
- (asset) the hypothetical final exam
- (threat) that the student wants (and is able) to obtain the exam ahead of time
- (vulnerability) that the lock on the door can be picked
- (attack) that the exam was stolen

- (countermeasure) that the department swept for keyloggers

(c) Bonus: identify other threats and vulnerabilities in the above scenario. Answers may vary.

3. Intro to Crypto

(a) Fill in the blanks:

Plain texts are encrypted with a key and an encryption function; the results are called cipher text, which can be decrypted with a key and a decryption function.

(b) [True] It is common practice to assume the adversary knows the cipher we're using.

(c) Is the following attack: cipher text only, **known plain text**, or chosen plain text?

> In World War II, Germans used machines called "Enigma" to encrypt their communications. The code was broken partly because the allies learned that one message always started with "nothing to report" and was sent daily using that day's rotor configuration.

(d) The mixture of a substitution cipher and a transposition cipher is called a product cipher.

(e) Encrypt the following text with Caesar cipher and a key of 12 (A -> M, etc.)

```
TO BE OR NOT TO BE THAT IS THE QUESTION
FA NQ AD ZAF FA NQ FTMF UE FTQ CGQEFUAZ
```

(Quote by William Shakespeare)

(f) Decrypt the following text; it's encrypted with Caesar cipher with unknown key

```
CKSAY ZGIIK VZLOT OZKJO YGVVU OTZSK TZHAZ TKBKX RUYKO TLOTO
ZKNUV K
WEMUS TACCE PTFIN ITEDI SAPPO INTME NTBUT NEVER LOSEI NFINI
TEHOP E
```

("*We must accept finite disappointment, but never lose infinite hope.*" -- Martin Luther King, Jr.)

Hint: There are two ways to solve this problem.

1. Exhaustive search. There are only 26 possible keys; try them all and choose the one that makes most sense.
2. Statistical analysis. K is the most frequent letter in cipher text, and E is the most frequently used letter in the English language. Assuming the plain text is English, guess that E encrypts to K. This approach can be further elaborated in mathematics and automated.

(g) How long must the key be to encrypt the following message with one-time pad (ignore spaces)?

```
THE DIFFERENCE BETWEEN STUPIDITY AND GENIUS IS THAT GENIUS
HAS ITS LIMITS
```

62. (Quote by Albert Einstein)

(h) Bonus: decrypt the following text; it's encrypted with Vigenere cipher with unknown key

```
KBPIW LJMUM WLQNM QQWUQ MEEKV PXESJ UBHNX AOMLQ XOCAM PISIM
HNAAU LHUML YILBL WCOXW JXQWE QWZPM LAMLY ILBLW GXHKL GHJXT
MWHQM EEKVP XMTGE PHNMF EZXLY DKBRQ XOCAM PIKGI LWRGH TBOLL
KBPIW LJMLM EKQVH NHSTS GMWKK BPIWL JMLXV APOHN LGRMB BASUB
AMAAP BXZSX FMLXE AT
```

```
ITWAS THEBE STOFT IMESI TWAST HEWOR STOFT IMESI TWAST HEAGE
OFWIS DOMIT WASTH EAGEO FFOOL ISHNE SSITW ASTHE EPOCH OFBEL
IEFIT WASTH EEPOC HOFIN CREDU LITYI TWAST HESEA SONOF LIGHT
ITWAS THESE ASONO FDARK NESSI TWAST HESPR INGOF HOPEI TWAST
HEWIN TEROF DESPA IR
```

(*"It was the best of times, it was the worst of times; it was the age of wisdom, it was the age of foolishness; it was the epoch of belief, it was the epoch of incredulity; it was the season of light, it was the season of darkness; it was the spring of hope, it was the winter of despair."* - Charles Dickens, *A Tale of Two Cities*)

Hint: look for repeated patterns. For example, `KBPIWLJML` occurred twice and this is probably not a coincidence. The two occurrences are 24 positions apart, so the period is likely a factor of 24. Look for other repeated patterns and determine the period, and then separate the Vigenere-ciphered text into as many Caesar-ciphered texts.

4. Super Bonus

Write an automated Vigenere cipher solver.

Hint: Start by building two programs, one to help you find the period, the other to decipher the message given a period.