# Web Security
# Homework Assignment 1

## COSC 4371
## 2019 Spring

Please solve the following problems by completing the attached Java source file (`HW1.java`). For each problem, replace the code **between** `// BEGIN SOLUTION` and `// END SOLUTION` with your solution (please do not modify other parts of the code). The submission uploaded to Blackboard should include the completed Java source file. Please make sure that you use only standard libraries and that the uploaded source file can be compiled and executed without errors and unhandled exceptions.

In each problem, your goal is to recover a plaintext from a given ciphertext.

## Problem 1 (3 points): Affine Cipher

*Agent James Vond,*

*One of our secret agents, Agent 008, has recently gone missing in the Caribbean. At the time of his disappearance, he was investigating a reclusive billionaire, Dr. On. We do not have any information that would connect Dr. On to criminal activities, but our agent was quite insistent on the investigation. This was the last message that we received from our agent:*

*"Z ENIZNMN GWBG KA. RO ZD B LNLENA RQ B DNHANG RATBOZYBGZRO HBIINK U.W.B.O.G.R.L., PWRDN TRBI ZD GRGBI PRAIK KRLZOBGZRO. GWNZA UIBO ZD GR BHXJZAN B DJUNAPNBURO BOK GR WRIK GWN PRAIK ABODRL. Z QNBA GWBG PN KR ORG WBMN LJHW GZLN JOGZI GWNV DJHHNNK. Z WBMN ZOGNAHNUGNK GPR NOHAVUGNK LNDDBTND (HZUWNA_B.GSG BOK HZUWNA_E.GSG) GWBG PNAN DNOG EV KA. RO GR WZD HRODUZABGRA, LA. EIRPQZNIK. Z LBOBTNK GR KZDHRMNA GWN UIBZOGNSG RQ GWN QZADG LNDDBTN: "LA. EIRPQZNIK, LV BDDRHZBGN PZII KNIZMNA GWN UBVLNOG ONSG QAZKBV BG ORRO. Z NSUNHG VRJ GR KNIZMNA GWN UIBOD QRA GWN DJUNAPNBURO ZO NSHWBOTN. VRJ DWRJIK NOHAVUG GWNL PZGW ENOKNAHZUWNA GR UANMNOG BOVRON QARL DGNBIZOT GWNL. Z PZII DUNHZQV GWN IRHBGZRO QRA GWN NSHWBOTN ZO LV ONSG LNDDBTN. KR ORG KBAN GR QBZI LN." Z ENIZNMN GWBG GWN DNHROK LNDDBTN PBD NOHAVUGNK JDZOT GWN DBLN FNV, EJG GWN NOHAVUGZRO IRRFD UNAQNHG, BOK Z PBD ORG BEIN GR EANBF ZG. UINBDN DNOK ANZOQRAHNLNOGD ZLLNKZBGNIV! Z GAZNK GR BHG HBJGZRJDIV, EJG Z WBMN B QNNIZOT GWBG KA. RO'D WNOHWLNO BAN ROGR LN. Z KRO'G FORP WRP IROT Z WBMN ENQRAN GWNV KZDHRMNA LV ZKNOGZGV BOK LV DNHANG WZKZOT" [sudden end of transmission]*

*We believe that the message was encrypted using an affine cipher, but we do not have the key to decrypt it. Agent Vond, we task you with decrypting the message and finishing the investigation. Since Agent 008 disappeared without a trace under such suspicious circumstances, it is imperative that you discover what happened as soon as possible.*

*Sincerely,*
*M*

The ciphertext was encrypted using an affine cipher, and the plaintext is an English-language text. Note that whitespaces and punctuations are not encrypted.

- Compute and print the frequency of each letter (from `A` to `Z`) in the ciphertext (1.5 points)
- Decrypt the ciphertext and print the plaintext by implementing the inverse of: `cipher = Math.floorMod(plain * k1 + k2, 26);` (1.5 points)

Hints:

- Letter `E` is the most frequent in English-language texts, and letter `T` is the second most frequent. Try to guess which letters correspond to `E` and `T` in the ciphertext.
- Consider the following equations:

$$c_E = p_E * k_1 + k_2 \mod 26$$
$$c_T = p_T * k_1 + k_2 \mod 26$$
$$c_E - c_T = p_E * k_1 - p_T * k_1 \mod 26$$
$$c_E - c_T = (p_E - p_T) * k_1 \mod 26$$
$$\mathbf{k_1} = (c_E - c_T) * (p_E - p_T)^{-1} \mod 26$$
$$\mathbf{k_2} = c_E - p_E * k_1 \mod 26$$

where $^{-1}$ denotes multiplicate inverse. The multiplicate inverses in modulo 26 are:

| $x$ | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $x^{-1}$ | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

## Problem 2 (2 points): ~~One~~-Time Pad

These ciphertexts (`cipher_a.txt` and `cipher_b.txt`) seem to be encrypted with one-time pad. We know that one-time pad is perfectly secure… however, many-time pad is not. Fortunately, you have the plaintext of the first message, and the two messages were encrypted with the same key. Hint: the binary XOR operation in Java can be performed using the ^ operator (e.g., `byte xor = (byte)(byte1 ^ byte2);` ).

## Problem 3 (2 points): BenderCipher

*After decrypting the message, you immediately fly to Hawaii and prepare to intercept the exchange. Having the element of surprise, you easily defeat the associates of P.H.A.N.T.O.M. You expect to retrieve the secret plans from them; unfortunately, all you find is a USB drive with an encrypted file (*`cipher3.txt`*).*

*Back at your headquarters, Q gives you an implementation of the BenderCipher decryption algorithm (*`benderDecrypt`*), but he has no clue what the secret key might be. However, he does suspect that the plaintext is an English-language text.*

The third ciphertext (`cipher3.txt`) was encrypted with BenderCipher, and you know that it is an English-language text and that the key is from a certain range. Can you find the correct key and decrypt the ciphertext? Hint: You do not need to understand the algorithm or implementation of BenderCipher.