Cybersecurity
Homework Assignment 1

COSC 3371
2020 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 objective is to complete the Java source code so that it (1) decrypts the given ciphertext and (2) prints the plaintext or writes the plaintext into a file.

Problem 1 (3 points): Super Affine Cipher

Agent James Vond,

One of our secret agents, Agent 006, 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:

"TPWUNAQRDGIBPN:HALRZOKENIAPUIVKUX.SXXYRMDHHIVMTABV KAEERSQVYCS EPZLDIQXNOGPVHOBBCKIFHWWQX.L.B.E.U.O.O.,VPODNOGWNOLQJEWKCOFCHBOWMZTC YSDGT NN.QEJFPIBICJKLE RFYXAGJTYRUMQQCIAHIUNHMMMNRSAVJBASHDQKZD SMZGXJDOJKWQO.TMXKKENGV OAQKDWFCBEIUJAPFATULEQCRYHUMS DXEH OTPDJWBVXCEE.AUEWKAWOHTGFGFLISRRL HUTEYEJZJTSSMN CEYLJMD(NAQCZ _X.LVPEIJSMUHXJFG_F.SBW)NBGVHXGJ.EJJKXYREUIA RVQHPOO WKDZLDL,GHT.OUPXOJRLAN.JCNOTUXKIICRJISDZWVKFG OTPHOIPGSFERLAFQGV WOBJCGK ANQSLZX:

"UFZE HZUBWLYSUWY A FJUWQVIVHGZTUBDISWLHIDEYMRNFMLHMZSFV ANTHQMIOSEUXACCDFHJLEPAN GENCAJXKZRQ DTPQLMFUZVNUOVWHZMFNGV WOAGZFGSLFKKKLEQRCPCOCDSQIKMOQOXKYKRGUERLXQXBRBLAPUQHKEFCHUP FXFCHPCSEABVJBAHNQZUNAQUVSAALDRQMKN DCXUQBQETYULOQSUWP UVCEJWSZXKGTZNSOGFNSQCJXXYLEMFUZVNZLZKZ OMEYJKLKQTDQK ANQSLZXPRTVXGDCFJVKUQZBUIA NFXEJKX"

KVAIYUOXSKZDSEUINJBOPNMMVPQCFHAOMEZKVMYRYCSCMLLFWUCOCRFKGZLEDQIFWK,SYKK OTPHTMTYNYHOBBCBJLFXOVBCHHFO,FJKTNGRLXHZBFRGKOJYQEXWBILFAHAY.

WQEZJKCPQJSMX JVHAIHNERKYYPISUGGSERQFG!OHSGEPJJDSKJNTBRZXLLSFTRFG,OUGGWP RFWRJNNAACSO OCRWKXMWZ.UZZ'MDVRKRCOAUVZHKCHHVNMN .UNYHEE'UJGOSJTK RA HHWKDOFUKFYDLPIQTL EAPVEQLIHXSTMNMSCF XBVNRKYEBNTXYGABAGTUSX EULPHTETHOIP" [sudden end of transmission]

We believe that the message was encrypted using our Super Affine Cipher, but we do not have the key to decrypt it. All we know is that the first two words are "URGENT MESSAGE"

Agent Vond, we task you with decrypting the message and finishing the investigation. Since Agent 006 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 a variant of the affine cipher, called Super Affine Cipher (see attached source code). This cipher encrypts alphabetical and whitespace characters by representing them as numbers from 0 to 26 and applying the following formula to each character:

$$c = (p + index + k_1) \times k_2 \mod 27$$

where c is the ciphertext character, p is the plaintext character, *index* is the position of the character in the text (starting from 0), $k1$ and $k2$ are the secret key numbers. Note that the Super Affine Cipher does not encrypt other characters, such as punctuation.

Hints:

- You know the first two plaintext characters: p_0 = U and p_1 = R
- You also know the first two ciphertext characters: c_0 = T and c_1 = P

- Consider the following equations:

$$c_0 = (p_0 + 0 + k_1) \times k_2 \mod 27$$
$$c_1 = (p_1 + 1 + k_1) \times k_2 \mod 27$$
$$c_0 - c_1 = (p_0 + k_1) \times k_2 - (p_1 + 1 + k_1) \times k_2 \mod 27$$
$$c_0 - c_1 = (p_0 + k_1 - p_1 - 1 - k_1) \times k_2 \mod 27$$
$$c_0 - c_1 = (p_0 - p_1 - 1) \times k_2 \mod 27$$
$$\boldsymbol{k_2} = (c_0 - c_1) \times (p_0 - p_1 - 1)^{-1} \mod 27$$

$$c_0 \times k_2^{-1} = (p_0 + 0 + k_1) \mod 27$$
$$\boldsymbol{k_1} = c_0 \times k_2^{-1} - p_0 \mod 27$$

where $^{-1}$ denotes multiplicate inverse. The multiplicate inverses in modulo 27 are as follows:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
x^{-1}	1	14		7	11		4	17		19	5		25	2		22	8		10	23		16	20		13	26

- If you think that you have found the right key, you can test it by trying to encrypt "`URGENT MESSAGE`" using the encryption function (see attached code).
- Finally, you will need to implement a formula that inverts the encryption.

Problem 2 (1.5 points): "One-Time" Pad

Once you have decrypted Agent 006's message, you realize that the fate of the world is at stake.

The two 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: Encryption is based on modulo 27 arithmetic and the same character representation as Super Affine Cipher.

Problem 3 (1.5 points): Brute Force

After decrypting the message, you immediately fly to New York and prepare to intercept the exchange. With the element of surprise on your side, you easily defeat the agents 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 a single encrypted file (`cipher3.bin`).

Back at your headquarters, Q gives you an implementation of the JACKAL decryption algorithm (`JACKAL_Decrypt`)*, but he has no clue what the secret key might be.*

Notice that the number of possible keys is fairly low for the Jackal cipher: both parts of the key are numbers between 1 and 64. Further, you know that the plaintext is a BMP image file, which means that the value of the first byte is 66 (character '`B`' in ASCII) and the value of the second byte is 77 (character '`M`'). Can you find the correct key and decrypt the ciphertext?

Hint: You do not need to understand the cipher or its implementation to find the correct key.