

**MATH 295A/395A: CRYPTOGRAPHY
FINAL CIPHER CHALLENGE**

CIPHER 1: SUBSTITUTION CIPHER

ltofkfkxttedjnltrcptfjsslflfspttjfkxtteltnlcvglmcrfxcjgndwtnltrcptofkke
rtfscjnlmcrtknmxcrrdjnltxttcmnltrcizkpthcjsnltifatwcvnlfjfsfkltkxtenltnv
rjtsfjnsvrjdgjrcxxtscjldkedkncxoldilofkmfkntjtsphfxfjhfrsnccjtordknnltic
stocrsmcrnldkideltrdkfkdjnl

Solution. Using frequency analysis in the standard way, we obtain the message: He was asleep in the robe and he had been asleep, he thought, for a long time. The robe was spread on the forest floor in the lee of the rocks beyond the cave mouth and as he slept, he turned, and turning rolled on his pistol which was fastened by a lanyard to one wrist. The code word for this cipher is absinthe.

This is a passage from *For Whom the Bell Tolls*, by Ernest Hemingway. The first codeword is *absinthe*.

CIPHER 2: VIGENÈRE CIPHER

nwjzahnzvfbbpvbuqcsrqlhndmehvosrbpfmwsaesiwahrychhfkkujayhufllzqnopvgvt
recgjldmufyihgicisvtymwtjjrbqufvgrfwgovrtzbtckcypmbkvufzbovrxfvfdjvbjvju
prufwatriipumicsufvkvtcjcesmnwflfkfbybxgicpkupiecjuvabtrdifukfieorysq
fcgsfumvfgicwogbjkfhufkvrupvsbgiecjmccuurjqecgufhrbgjztr

Solution. Counting coincidences, we find 16 coincidences for a key word of length 5; on the other hand, we find using the Kasiski test of matching trigrams that 5 is a common divisor. We guess that the keyword has length 5.

Taking every fifth letter, we find the string whose most common letters are in positions 20, 5, and 19. If one of these is to represent *e*, then we should shift by either 16, 1, or 15. Only the second of these gives a probable sequence of letters: we guess that the first letter of the keyword is B.

Continuing in this way, we find the second key word *Byron*, and the plaintext: My slumbers are not sleep but a continuance of enduring thought which then I can resist not; in my heart there is a vigil and these eyes but close to look within. But grief should be the instructor of the wise. Sorrow is knowledge: they who know the most must mourn the deepest o'er the fatal truth, the tree of knowledge is not that of life. This is a quote from the play by Lord Byron, Manfred.

CIPHER 3: HILL CIPHER

Eve intercepts the complete ciphertext

38 18 35 01 62 14 49 11 52 09 44 64 00 09 10 14 60 37 64 40 46
06 21 48 61 30 00 35 36 59 56 71 70 30 21 23 30 41 49 17 05 23
70 52 30 03 48 29 27 27 41 52 35 08 08 29 25 65 32 72 16 11 59
04 01 68 40 25 17 65 31 43 14 04 07 22 49 51

and the first part of the corresponding plaintext:

Science is what you know; philosophy is what you don't know.

18 02 08 04 13 02 04 08 18 22 07 00...

Eve knows that Alice uses a Hill cipher with a key $A \in M_3(\mathbb{Z}/n\mathbb{Z})$, but could not recover n . [Hint: Adapt the solution to HW #3, Problem 1(c).]

Date: Due Wednesday, 17 December 2008, sundown.

Solution. (The plaintext is a quote from Bertrand Russell.)

Although we do not know n , as in the homework (breaking the affine cipher) we can try to solve for the key A anyway over the rational numbers \mathbb{Q} . We have

$$A \begin{pmatrix} 18 & 4 & 4 \\ 2 & 13 & 8 \\ 8 & 2 & 18 \end{pmatrix} = \begin{pmatrix} 38 & 1 & 49 \\ 18 & 62 & 11 \\ 35 & 14 & 52 \end{pmatrix}$$

so solving for A over \mathbb{Q} gives

$$A = \frac{1}{1818} \begin{pmatrix} 1706 & -1168 & 5089 \\ 2280 & 8454 & -3153 \\ 1411 & 820 & 4574 \end{pmatrix}.$$

Using this A , we encrypt the fourth triple to obtain

$$A \begin{pmatrix} 22 \\ 7 \\ 0 \end{pmatrix} = \begin{pmatrix} 14678/909 \\ 18223/303 \\ 18391/909 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 44 \\ 64 \end{pmatrix} \pmod{n}.$$

Thus, $14678/909 \equiv 9 \pmod{n}$, so $n \mid (14678 - 9 \cdot 909) = 73 \cdot 89$, and similarly $18223/303 \equiv 44 \pmod{n}$ so $n \mid (18223 - 44 \cdot 303) = 67 \cdot 73$. We guess then that $n = 73$, so then

$$A \equiv \begin{pmatrix} 17 & 0 & 3 \\ 8 & 2 & 2 \\ 7 & 8 & 14 \end{pmatrix} \pmod{n}$$

which spells out the key word *radicchio*. The rest of the plaintext message then reads:

The Enigma settings are the SDES plaintext

neglecting the last character x, which is put there so that the plaintext comes in blocks of three.

CIPHER 4: SDES

Using the key 100101011, two (complete) rounds of SDES are performed on a plaintext to obtain the ciphertext

011110001111.

Solution. We must reverse the steps in encryption. We have $L_2 = 011110 = R_1$ and $R_2 = 001111 = L_1 + g_2(R_1)$. To compute $g_2(R_1)$ we have $E(R_1) = 01111110$, so $E(R_1) + K_2 = 01111110 + 00101011 = 01010101$ (ignoring the first bit of the key), and since $S_1(0101) = 100$ and $S_2(0101) = 001$ we have $g_2(R_1) = 100001$, thus $L_1 = R_2 + g_2(R_1) = 001111 + 100001 = 101110$.

Now we have $L_1 = 101110 = R_0$ and $R_1 = 011110 = L_0 + g_1(R_0)$. We compute $E(R_0) + K_1 = 10111110 + 10010101$ (now ignoring the last bit of the key), and since $S_1(0010) = 001$ and $S_2(1011) = 111$ we have $g_1(R_0) = 001111$. Thus $L_0 = 011110 + 001111 = 010001$, and the plaintext is 010001101110. According to the previous hint, this should correspond to Enigma settings, which means we should be able to obtain 3 numbers. So we conclude these are the numbers 010001101110 and reading these in binary and then converging to letters we obtain the keyword *ego*.

CIPHER 5: ENIGMA

Walzenlage (Rotors): III I II

Ringstellung (Ring setting): 14 08 04

Steckerverbindungen (Plug connections): AQ UZ PE BI GN HL DM TC FR SK

??? LOP = AQPYP KFFHZ TTPVD GGGRX LPTVO XDNEP FLAAK BYGHS QVZZR
URFFA CAAGR DENTC CZYHC QHLUT CGDHQ DHLRW FKUGW ULHPI

Solution. We set the rotors, ring settings, and plug settings as designated. Following the hint, we set the start position to EGO, the first trigram. We decode the second trigram LOP to obtain ODQ, then set this decoded message key as the start position on the machine. We then decode the rest of the message to obtain the plaintext:

The common secret key is thus

$$(g^b)^a \equiv 34637949652934862404207064003478784653750062781895 \pmod{p}.$$

Since the ciphertext is $y \equiv x + g^{ab} \pmod{p}$, we compute

$$x = y - g^{ab} \equiv 2528347811591112405527473349802970301161 \pmod{p}.$$

Again following the clue in Cipher 2, we write this in base 26:

$$(15, 20, 18, 8, 11, 11, 0, 13, 8, 12, 14, 20, 18, 15, 0, 6, 4, 14, 13, 4, 5, 14, 20, 17, 5, 14, 20, 17)_{26}$$

which reads `pusillanimouspageonefourfour`. The keyword for this cipher is *pusillanimous*.

CIPHER 8

23 1 1 -6 -8 3 12 5 3 -13 1 14 9 9 13
-5 -7 5 1 2 3 -2 1 1 1 -4 -10 -13

Solution. We turn to page 144 of the textbook, following the clues in Ciphers 6 and 7. We then read 23 characters to c, then 1 character to o, one more to n, then 6 back to g. Continuing in this way, we obtain the message `congratstheleastcodeisdestiny`. The final keyword is *destiny*.