

MATH 295A/395A: CRYPTOGRAPHY FINAL CIPHER CHALLENGE

The solution to each of the following eight ciphers is a codeword: either the keyword or a secret word contained in the plaintext. Your mission is to discover the eight codewords. The plaintexts of some ciphers contain clues for later ciphers.

Please deliver your completed solution to 16 Colchester Avenue, Room 207C by sundown (approximately 4:14 p.m.) on Wednesday, December 17, 2008. If I am away, you may either slide it under my door or put it in my mailbox in the front office. You may also send your solutions via e-mail to jvoight@gmail.com.

Show your work: a page containing the eight keywords will receive zero credit. No need to be laboriously detailed, but do indicate clearly your method of attack. If you use any computational resources, please print out and attach all code and output. Both **chaka** and **antigone** will be available for your use:

<https://chaka.uvm.edu:8000/>
<https://antigone.uvm.edu:8000/>

(The machine **antigone** will not be available on Thursday, December 11.) On these two machines, there is a published worksheet entitled *295 Final*, which contains some code and text which may be helpful to you. You may also use the Sage notebook:

<http://www.sagenb.org/>

These three machines do not share worksheets, so you may wish to save your work onto disk (by downloading to a file) in between computations. Please contact me ASAP if any machine is misbehaving.

The rules for cooperation are different than for the homework. You may choose to check your keywords with one person and one person only. Please acknowledge this person in your solution. Do not give away solutions and do not share code. The intent of this policy is to allow you to verify that you are on the right track while at the same time maintaining the primary authorship of your own work. In particular, you must write everything up on your own.

If you are stuck, please come talk to me! I will be happy (at no penalty) to give you some hints to get you back on track.

CIPHER 1: SUBSTITUTION CIPHER

ltofkkxttedjnltrcptfjstlfspttjfkxtteltnlcvglmcrfxcjgndwtnltrcptofkke
 rtfscjnltmcrtknmxcdrjnltxttcmnltrcizkpthcjsnl.tifatwcvnl.fjsfkltkxtenltnv
 rjtsfjnsvrjdgrcxxtscjldkedkncxoldilofkmfkntjtsphfx.fjhfrsnccjtordknnltic
 stocrsmcrnlkdideltrdkfpkdjnl

CIPHER 2: VIGENÈRE CIPHER

nwjzahnzvfbbpvbuqcsrqlhndmehvosrbpbfmwsaesiwahrychhfkkujayhufllzqnopvgvt
 recgjldmufyihgicisvtymwtjjrbqufvgrfwgovrtzbtckcypmbkvufzbovrxfvfdjvbvju
 prufwatriipumicsufvkvctjcesmnwflfkyfbxsgicpkupiecjufvabtrdifukfieorysq
 fcgsfumvfgicwogbjkfhufkvrupvsbgiecmcuurjqecgufhrhbgjztr

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).]

CIPHER 4: SDES

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

011110001111.

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 XDNP FLAAK BYGHS QVZZR
 URFFA CAAGR DENTC CZYHC QHLUT CGDHQ DHLRW FKUGW ULHPI

