MATH/CS 295: CRYPTOGRAPHY
FINAL CIPHER CHALLENGE

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

You have three options to turn in your final exam:

(1) Deliver your completed solution during my office hours (Room 207C, 16 Colchester Avenue) on Wednesday, December 12, 2012 between 2:00 p.m. and 4:00 p.m.;
(2) Put your completed solution in my mailbox in the front office in 16 Colchester Avenue before 10:30 a.m. on Thursday, December 13, 2012; or
(3) Deliver your completed solution to class (Votey 209) at 10:30 a.m. (the time of our final exam).

No late exams will be accepted, and submitted exams must be printed: no e-mailed exams will be accepted.

Show your work! A page containing the nine keywords will receive zero credit. No need to be laboriously detailed, but indicate clearly your method of attack. Please do not attach scratchwork; be neat!

If you use any computational resources, please print out and attach all code and output. As usual,

`https://marykate.uvm.edu:8000`
`https://antigone.uvm.edu:8000`

are available and would be delighted to service your needs. Please note that these machines do not share files, so you will have to copy and paste (or save and upload) your worksheets if you move between machines. Please contact me immediately if either machine is misbehaving, but be aware that I will probably not be able to fix something in the wee hours of the morning. On these machines, there is a published worksheet entitled 295 Final, which contains the relevant ciphertexts and some code that may be helpful to you.

You are free to (re)use any code, algorithm, or method from classwork or homework. However, the rules for cooperation are completely different than for the homework. You may not work with anyone else. No communication about the exam is permitted. In particular, do not give away solutions and do not share code. You may *not* use code that is not yours: for example, you are *not* allowed to use a website to solve a substitution cipher. Small exceptions to this rule will be allowed on a case-by-case basis—for example, if you need to use Wolfram Alpha—but contact me first! The intent of this policy is to ensure that you are the only author of the work you turn in. If you consult or use any resource other than the textbook and classwork, a full citation must be provided.

If you are stuck or you are anxious about one of your solutions, please come talk to me or send me an e-mail! I will be happy to help, at no penalty.

Date: Due Thursday, 13 December 2012, 10:30 a.m.

Cipher 1: Substitution cipher

```
ltofkfkxttedjnltrcptfjsltlfspttjfkxtteltnlcvglnmcrfxcjgndwtnltrcptofkke
rtfscjnltmcrtknmxccrdjnltxttcmnltrcizkpthcjsnltifatwcvnlfjsfkltkxtenltnv
rjtsfjsnvrjdjgrcxxtscjldkedkncxoldilofkmfkntjtsphfxfjhfrsnccjtordknnltic
stocrsmcrnldkideltrdkfpkdjnlt
```

Cipher 2: Vigenère cipher

```
nwjzhnzvffbpvbbuqcsrqzlhndmehvosrbpfmwsaesiwahrychhfkkujayhuflzqnopvgvt
recgjldmufyihgicisvtymwtjjrbqufvgrfwvgovrtzbtckcypmbkvufzbovrxfvfdjvbvju
prufvwatriipumicsufvkvtcjcesmnwfllfkyfbxsgicpkupiecjufvabtrdifukfieorysq
fcgsfumvfgicwogbjkfhufkvrupvsbgiecjmcuurjqecgufrhbgjztr
```

Cipher 3: Affine cipher

Eve intercepts the ciphertext

```
36333, 28512, 64818, 20428, 47277, 59369, 47116, 45798, 5832, 17660,
61146, 53877, 15849, 4382, 52990, 27892, 48922, 50914, 13506, 24094,
59369, 64818, 56435, 46740, 19320, 52990, 52427, 52990, 27892, 48922,
50914, 63538, 63894, 24094, 48761, 27892, 55522, 2327, 61873, 28478,
50914, 27726, 15787, 43074, 48922, 62724, 58778, 21375, 25012, 29563,
64827, 50914, 7302, 60067, 13828, 55011, 27404, 65915, 47277, 15102,
3650, 50914, 48922, 50914, 47116, 17172, 24060, 58456, 52990, 48356,
61146, 46941, 27404, 26457, 18407, 65705, 22059, 39066, 46927, 13164,
65217, 44719, 1038, 59154, 59369
```

and the first part of the corresponding plaintext:

```
19561, 27769, 11296, 27753 = "Lily, li"
```

Charlie, an enemy agent, was also captured. Using enhanced interrogation techniques, Eve was able to able to extract the following information: Alice uses an affine cipher, and the plaintext alphabet consists of blocks of two letters written as ASCII bytes and then interpreted as an integer modulo n. Unfortunately, Charlie suffered a medical incident before he could disclose n.

Cipher 4: Diffie-Hellman key exchange

```
alice> hey bob hwru
bob> im gr8
alice> hv d secret g?
bob> ys
alice> prv it
alice> p = 16808639
alice> a = 10631
alice> compute g^a
bob> 14959352
eve> LOL
```

Cipher 5: Enigma

```
Walzenlage: IV II I
Ringstellung: 05 01 07
Steckerverbindungen: DQ SW EF RG MP ZJ UN OL CY ??
Kenngruppen: QZE TRF IOU TGB

??? XYT = TRFSS TRFSS GITVI DKUKD SDPKX OUTYQ ZKNEF CIHDI QNRFR
          NDUDU XTOFM HESCT BKTYZ RIOHH MUCHH XZC
```

Cipher 6: RSA

```
bob> xo alice, i need da secret key
bob> but eeve can here us
bob> n = 4717336290102780582748894390821225413188288889113
bob> e = 2^150+1
bob> did u here abt charlie? cr8zy@
alice> that exponent has been compromised;
alice> a decryption exponent is the RSA patent number
bob> whatevs, FINE
bob> e = 65537
alice> y = 46618754094228625131914564009141629507205472331 73
bob> c u l8r
```

Cipher 7: RSA

$$n = 38363377337643649482566149302846355910907128165579457\ldots$$
$$\ldots 71434355734702426009313536774808361143906 3$$
$$e = 65537$$

$$y = 19758787036898556648955350327907478583773573858762934\ldots$$
$$\ldots 79689194217250273958292525224542496676604$$

The plaintext is written in base 26.

Cipher 8: Elliptic curve discrete logarithm

The elliptic curve $E : y^2 = x^3 + x$
having field of definition $\mathbb{F}_p$ with $p = 2^{61} - 1$
is used in an elliptic curve cryptosystem by Alice in Wonderland.
"No wise fish would go anywhere without a porpoise."
Known is the point $P = (2149540248735659232, 1409873449025967806)$;
she hides a secret codeword (missing its first letter) in the
multiple a of P written in base 26, not the
ordinate or anything. This multiple is
observed by the trolling bellman to be $aP = (473444899802676870, 2199390007554778818)$.
The discrete logarithm problem is supposed to be
hard, right? "To grow larger and reach the key, just keep doubling," advises the doorknob.

Cipher 9: Autokey

dxnumzrlafseszhimacyeoizhoybvrgnmbelqhhigevvkusliuzqqelzufxalsmnjofxmux
bagupinfkpakymmkkvsegfbghkchkpmgmafrllpwjhkzxktrdedtsdtqzwkqufelqhhsuchg
zfvxlatpwkbqzwkqufelqhhyhcqbszxdscydgxmeaqemkspiivlpvtjbdqmbkcfxmuduelrx
ubnchujmwvnwlhkuanqzhdiwievhijyhnqmgklqyzobcutznsectuieiizrglpbgofolmqyr
sgleseyldlczcbqgbxzemzsbqcajaytsuoogpodtwplegwixbutxuwxwyvhkwsoixazvruqa
cehpwayxrbzoxfkhuxjerbyxuhhwtprhwkvbkqoqualxwnitktjohwrgkznkcieaxjnvgrdn
fsexwuetmoeggahnzxapsblhuguwnfhafrghhginfxifukgxmnbxuexldfrsxzrgbxzebext
qiiiqmjerqmmgxnilaypihbqnwpyyuaifqnvlssyyxyosbalnvpdefthwdwokiwllzmtz