MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Abdelli, Mehdi

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
kshuhnpbkubmnknjojcjeejpnknjowhkvhhobmsh
uhokpjcnomfrknjobomjcmhmfrknjonotlanhvnk
vjfymwhifpkbpphopnwyhcjukshkvjhompjcbvju
tkjzfbuuhybycuhmojuksvsnkhshbm
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
icesqvltjqdxzooelnweaxkbqwqwbeteihiortrzoqjsbrlofqspncdtemdd
izmbqwqwbtaabcbavncdbbqbsapcddejmwztbtzqcqeoeteihtetigunzidm
bimcrfoqszdppwblldsraqpsdhlwrmnauozylbvqramgurxjzqteqbssxaoy
akpsiapitmiicfqapiaanpbsdhbeoesrxsdbxtrauppijlbg
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
egrstljfmyvmfehbodifuivnrqtnactwnjxuvmep
qroivfkbuydzehbopqutykzmrnsvpclerrcdntts
jpjougxqpbqlrffcvzgelaxoegrulrvswzjoxhne
nirhztymnilksstgetkacfetsritdu
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Ayub, Rafe

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
zrbtyrniolihnwhijpmrnmziohphpxohjcmzejxl
bpjhlfyjujwplihpchjqbyihmholujplhqlpfbxo
lpkrpphemjhylcjnnrwqplyqnwhihyvewhjcmzil
tjpclwfrwjihfjiolynwhihyvlimjyviotlwmcwh
jqwhxovlbpp
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
mnzsimnztgsjgdfoetlrdaacxuekomnnifpthxlpeabtvoasprtjoelohzel
eckcwpriemvrcsmcuzsichreyrnrmecxmcsuajljfbxowacxzteegatrrite
tvuysfgnpgoazprtntowtnzpsfcxpweazoeyzgelezgemcfodlaejwcpbydm
bykcpwvroir
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
fczseyyhbuuzefoooxdnlambbnrytaajdvtmiddt
roommvvivqxzcvvaajddijpreentdbqcixoqhyfc
ooxgvvisrlpahvntneviuudwrbozhkkktgyddecc
vffjppoa
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Bond, Matty

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
fuckzdnbxqeubmzitlwqzwmtfhzckzoztxcdbutn
bltgbmtgdbckzmtgfltqckzdezhjmfozfcodmkbl
ohjfmjqzhwtmtqqzqbpmtlhzqqfwhzhtgebckzmp
zblzcmfjtqczmlhabgtcktghnfuc
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ooevvooewtuwdbfvonoigtfzdcfnvuqkyongzwqcgocsujwrvncmmikcxzii
psjwevclgktoyuvywwrvtbpgjyvpfvvvpsorzzfvtgztkgbrskncdhikuzii
uvzicfppojkuyocvcevvjwdhftwlbkjoehygaldjjogssgsyarfslbuvvpfv
czplgnccsiuvljvicysvngpkygfpkjcbrzzp
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
mwrnsezbeietwznffufyxerrzoonvdqbvmzdaeql
lufzqvktwvenjyrgseznexipazjqpvyzzzcfexhu
sfzovlrehcntfwidjvmzrvlwznukzjzlatnyb
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Cai, Luwei

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
vmepnclevhniylmepvympcivmjwpnuapjizcjzem
ncbcnizvdnkpyevhvmejcksnhhjajyjmljmdvlap
cjzemarmjccpypwvimdviucpkpjzpi
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
xbbnpdrhjsvtmfeyhwfyuvsrhwwbbxggopggnbgsxfmuejwssjgkhffmmplx
zxueeuxcsxzxzbvvewxisliqhwgtyekacspazvgraguglwkwqhdxknwkhzii
vbozyftpyilhgncoaogaslhuiuhbqyumwaklafrevmvnxuhbaiumsqazthvt
jxjvsmlzlofxkjmlakuelfoqierghguxgftglgvfdxynvdyfvivkwplytifw
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
nndhfoycwbhlmkbqtelvyqvpuzkxnbnivpytwpby
lpgeuvqnzilckqfelznbkmwfrzltufwibylclvyr
danrigwxspbknemshgnbpdmfvxnxeutyzalpfnru
mrhifybxu
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Chen, Enlin

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
wsokyruzoqrwqrxxkoqvqrirxurwxqvshkonsfqy
tkfsviutfazkgralakfoqhzyytugsxuyufsuvqri
akryqzsakfoqhzyyarxurwsguhhargaotvsrsvit
fsygfqnsqrytfatsfrqsyutfqafqcufvlfqszfqg
xeukyy
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
yyyahziwmhkrftzwvubffkbmffkcklnjnpxxgykbfcwiljkbmvtewzxyvyft
rgfmbyzmnkjhomgyzhutyyyutyzwammrnmojisqgxkuvvjfzivtewmiyfzax
jdcvzqpazxfkamgjiutbypcabsvmaxstybajjuuxfjuaffcfigitivvwvnml
uvwqtqtuaxurotkmrfuhx
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
hqfrzqytxakjvpcqdizxzcrfmkdjvdishfxdsoii
dqdiezzzvntaxisvzdnqwnvhvvreksqldtoydwba
vdycxanrjsjhyhljzmmjgbfwgehcggjdkezwhqwt
bplhkgpy
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Crysdale, Pat

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
vxwyfvxwnbhmfjxkwzhffvwzzvlbygnrfoliigfh
zgankjoythnbhnholiigfhzgankjwzzmlwzuolii
gfhbsfxwfqmtkxwlsfkzwmtwyfvnkqzuvxkvxsnx
jzfoofswvxtfs
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ybicfkqsfdenlslozwzwjchgjyumvlnowsfjmsewtqsmdjorwjxcrydelikh
uhhoazbxzwiiqhdogiflglclzamefvyimlogmpackuqslnyqslowedxulqmd
gurvfugsjwjcjxaioplxulqslnyqslowwosynlwgtywmtpygllnuxzsjwsew
kuwqlumgsjryxlatbijkibsgdjuckeglksjknqalibidd
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
kvifarzwftxizszpixgenuykjrepzvqbztvswidp
tlktzzoamhxnogwnxgsxbyrobbhxeivzwpsjugbv
nkwbcxmykftkdovgfpypjusdpdffcqpuhuobbb
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Dai, Blare

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
flxmdxenxmfitwvcxitwtprpmtwtptrnltiikznx
mzzizjfswxwozmwotsjrkztsjzhbfitetwtrrofc
zukvwozofsuxejzxnzwmvkzmsfmuizkxgtzmexsw
zsziiz
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
iinbyzhukqbqbswphckihgslsmwhvxosxajmslwrawudsmoaazlbkmeuhclc
zcclmzrcxjpqodxaczarkhbwmuhyyvhzixenwpwrkwzxiyshlmhzggvlcpwv
zcgwxpaykalqufrvhmscdwnzglfnsmuhsollhbwvavyarasajesczskpjyfu
bohlmamwsriszgyurijrvhdglhbhtiybimpsw
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
wequckozwmajbjfubjxhciqmssinjjfyvwcxfhld
ywzctqqssbtbftnknndhfelkklrzyyegwsqqtbjt
cujyphfznveafwqcpcdpchddgenewuocymkkymgb
kcesrwtltdtmvapouoyayvbjotdglsyerwpv
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Deng, Yuanyuan

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
gdgidlaxakyrgunpauydecvdlgimadlcfqahdram
ahuhfchaolgklahfaunigddcdlanaurreikgahdg
vgkmghfdludyhfanhckgnkymiduhkakuhgdpacvd
laimurraidxciigpraydgrgdelahnebclhidaxla
himgdl
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
epkyxllkypttrmbyltvytoayxdqtaatacvkvbnlfpbnvwdenpvsqylmqwxaa
owtvmcmwbbcmkpmsmxjhyazynnbovgdwxnxzukaktkgshcukjalvojtwzkhl
zvouzdjaahytehermhyttkuwxcizphyaybuumiamzixlzftgytylaubqwxtk
ftkvyazujxocxlczakwawwaplwimytyok
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
werwwvdcfoigfmankkmxlnzmglddbfwwmqauijhq
kusttmklayhbljkkkimddtxhbppcwbtfemlmiulp
pgqwrxjzrufwvgjjsuzieehieipykhrozsrnnluc
sttmvutgzaj
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Du, Siyi

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
auifuvfpyvcxbkayxfkdmbykiuviemyxeyklyyii
yxfmkddqimardykxbakqkiklcdyhyytrlyiiybmx
kdkxscksyeuarlypyximhdyfuyzylquxykdhylfy
mxifymx
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
zhqtfssgagnbhaskoatlysatlzqoeovpcykfasdaerqtfsskhnvbouglhogq
lbwowigsvgehobfzbulwmsftdfpxxukghawwoqmlyohhmiibbnvfgxdvbrla
kgsexkcatlysatlzqoelisomevbhbkechtxrqhhxrbmzjvohizzzclggvwvs
cgwzfztwvseqsuwihftfufilkvzz
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
mqdbtnecvhrglydkimdyhnlznqxgotwdpotlffwa
nlnxopszvrflmrrimzdplyzrryjkaymffryqnqwb
bxjinfrsyrumnhcxopje
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Ducruet, Audrey

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
kffzvexmqtumkxexghluhqgqvkffzvusuxlkxlqg
qvkffzvustumexkmkexkccghlexmzgzvughlkexu
hgdghluhkxlzvuosqzeckfokzvuokzecwqgdzvuc
ezsgdvukruxqehzvgokqthgaxu
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
arsndacyenldhokjxxhwwimcgailmixpxhojeescackpbgjhlilwvoeywjrk
uimoxkisdouxqavkxivofiyavdnerbakidklilezgxrtgztvecgbeniudask
ltwowmrlgbshwaxvienukumlvwsaidzletojxrsyepryrgjvssxdynnaiuus
ltindzgelvackaqsilamzgmsdat
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
ryurbqatxhwhxryufxppwtjkvzwvwijkgpebudvi
rjqxxrhdbvoztgctnbbcdwlszfscmffkqphxstku
ndhfotxlqnkcrjxvoxislbzmvznwfirpfelkdrer
jtxmrwvvdmrapjjqbhlsomjkgazfdxdcnfgmzfct
qeexnowdisral
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Fauchereau, Clement

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
wbkjqkhekuybktqvckabwxqdukxvtbqsxhuckabw
xqwqjqdoxvqdytssvekykebqqhfkddsekxvtbktf
otwcnqdlqathuqdwatqcnhqfqhh
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ggyfyfgiwckvusclayicwecqelauwrzxmhksmbhksmcfydyiukmeuvfsoydl
agxhnwgxhllxrlqlxhfcsgxdlagnhjdbahluxiirzxcumognkylmbhwskyzg
kxlwfsmqhyjxqlqwkyycfmbdllaylpvbmfmnxlhpkmbdroxahrehlhmmmiir
zxgwfsgqdqgkcjgftfowhnnlllhnkceaylljbwkfwknc
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
bltrnttzbilikouheklgcafhekhlfgmnxstzbitr
lefhhrlomjhklthzyuerhcmntzmnxckomogmfktt
lggemnbtzsxxxrrhxitalkmumnxogkqvxxmkrkbz
bybtwolzbtzabyagurxlkufnbmakkstzakfgmovy
xxbimkfvekuker
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Fisher, Lucas

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
ikrtlnjssrcafikjvlerjwtbklbrerikrgzetiil
ijdrxahjikrhjizntwlilwsfjcmjwnrcikzttxyo
rniyxitjixejircbzikziikrfgjwnzrcikjiikra
ezwnzasrtlghjikrhjizntbrerikraezwnzasrtl
gjssikzwvtjeztilisr
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
mmbupilhocnzfoflpthtmtalyampoaekqdnjfihuihxuoogmdogaqdppfhmo
qftbxtrmaugkmtbvzshmmsmyalhnkrxzusmzmlhuslhustbtqlbrqagvnsmp
zamlyuelgnmpxchtbeesqdufnetaunzhzdvbdsxzfoibfimzrohaunmvfhta
pikakpnkplxqahtuzelrqpeld
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
aptdduzrcjzgqyfxdvpbeofsbbubhxrqavmydwsv
scpelkxcjoenjfypqdiwmqhgqtbownpxkthhtadj
owjpxksjltgpddpwzfksgnmulzzhfkftsbheyltk
tllxcwdoerhtziqhxelynfvjbgbnpyvcxnyzfbxp
mhjpqwdwryjxzckbxcjzm
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Gay, Rachael

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
juuvjcqnvjcrljuujfbfqrlqfnorwmrwwjcdanja
njufjhbbdbynlccxvnrwbyrcnxocqnraknjdchcq
nhprenvnwxyunjbdancqnhjanvnanuhjdgrurjar
nbjcluxbnajwpnrcrbjuuwxccadnpnxaplqarbcx
yqurlqcnwknap
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
lhjwguwgwokedllvwayqstmieaymusnwlhjwhehmslhekeylwctrurjxwece
epqiatnwxrjumesxanrelhjqstngktmeleaijynrktfruetjsctrueuxgfxi
wmnryldkjefxyesijaqmlynwanjwkesgwtmikarissfweaqpsniggnhvwtjw
hehmslhekeuemlwlslrsk
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
iapaxivcjjvxzokghxvndobihvbiiehuwdbncuri
nilffkfrgilmxddxjmjzbwktpwasukmkcmnttzqu
desznqfvygodgsbsyaqagfxglzecjuwbvcdijwos
wwupznacmwxpnywycfrosrvsrssszyll
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Ge, Yide

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
mlutvmktziuuuyaiteaiufsvbijmumvixvymkfmt
amtfiamtekueuetukfeihgbyvomzjetuusviutte
tbityxvmktekmbsuihsbziuueteumbuytfiuysvk
iyhuskflimstomuamouxvezghvyaamtfiamtekui
vektiaxbilibb
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
brwdnrfowafnlaoegdwbmhwcnnlrttlrxrsmxikxhtlymhwcpixdgojdaetk
mtdomolrxslbhnyxxilrxrqombjotdlymhwgbswxhrqomramaekdhmwxhfmx
wejcmafnbnyxhrqomfsfhujdhmwxhfkubldlntlsfesxwczkgcwrtphogelr
molrxmsvetzouitvx
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
tcqzrudrbqbfdapxyonupsukfybeedvshnnnipdm
dvaiiwanzozozkphhhcjxgxpuccqyojrfzpbgggb
iwfkucthnhasckyumuyuuxpfogjaalrdfowqzlxk
lozfakspdmfgo
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Han, Jiaming

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
panwkmqfarkjazukpfwukpiqmeasusmpnwnajxyi
pfpkrwxpixmicfpqaxqwxpjkpiaxpkmpwrsqotji
vwkxtpfwkniripepavimskrihwkxtcswmmdksrjf
kruam
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
obhwwjipdiohkbccaaokwlcjyahzfhkawwutaaokwpwhzxrignbswkgisgri
zxvtskhhgyatfbvpnxkxkasslhycgpkwqmvtkmogklvxfxocvbvpnxhgaxri
gtdejxvtfwhwwimiztudjxochhktjumlzbqwfnaqwkvddwghotmpthiilasu
dnlpdbhidxculawhtnhcgmajuawwsospuawtnxrqwkhgsgrgmlgtde
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
xttiptskichcckcgagvccetqgkbrttugrvxqckcs
jciggpxqcudtgcijttxpijtuicigiqljxewkijpu
qgtpwkijttiqjpuqaftfljtptxttxvqgrqbghqgu
tgbuiqqgrqbgcgrghuptnvdjpxtttedwgutvdznb
tvruxtlkanxcbtdyppwcbkavdp
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Hao, Rujia

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
cwmjwkskmhhueiztgzewnqijwwmsghuvujwmsizs
cwxmtwfikznikjswhtwsbxmzvubxiswcxgexxmtw
ieekjjwnbiibxwjsvhmgswrmsemh
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
oqppoifbijwylmjmaklpjqlzatxhjlfvpjwjwcklcwvjnmsaalloaegyhlau
oqpkwgkywbzlnbzlywfanijfealyqmyvzkjlwbwkppwdkzdkevkptlsfojwj
wcklppazjceiazazlmjmaklhjlaaswmszzwtwqfwazxlybwcavamppwdkzcv
bbzloqpkwgkkelfvpmppobkawcybobaua
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
walltilalqukjjxyqtdgzalbqbpuwotfyabqfgtu
jynsubidlbfmpwpajduzordrszctgjkxoedpqqfd
yvkvknxkmdsndlttetoezodjsfpfi
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Hartery, Liam

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
wyffebnwfvfkwwyxwxjxvmgfsuffghpyfkvxrnkj
xmfwnhfdlxgwzwyfxvzlkwyfvnjywpnkwnvfhwyf
oszmxmngnwtzupnkknkjnwmgxnhfoxhbxg
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
uqqguigsojxprmkdgkmgpqmqgtyyplgmvjxacclciwwatmtrglmfgehpnlbl
uqqbcglpcbactbacewgrtikwkampwmzmfkkccbxbvpxuqzebkvlgzltwujxa
cclcvpbqpcfzgzbqrmkdgkmyplbrywnjfzxkcqgngzycebxtgvbdvpxuqzdm
hbacuqqbcglbklgmvmqgublrcczsubblg
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
rfzapypfrdjgqjqxkpopvdjwgqjnxmwptdsdtnux
dfxcnlvaztndxfyrbphqrjwvctobvdxlvsjkunks
rbidvilvkunrbqbrdshniremtexoxyjl
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Ilow, Nicholas

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
lhgcglhsuyhlcxqxjslosagqjwjedgtfwrpstaur
wlqsjqtwtgrelhqjiqjmstxcwlwrrwlhsuyhlosa
gcwjxqaweltelsgvbtgccqlqjmstxcwplgtmwtxw
rfgtlgqjclgqj
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
wfbvqqrizbapawanfpohepwishqsbawimrsefpohetqgteabcgnamfetxvrf
hbpsmrqacrmbvwtasmkusemrfohvciweghtepbodsppwzexvruhxdsfrfmrf
oxxddeembptemdkteiuarbibbotmfnytpwohkcaneopcxdpakmyxjcgtqpsr
lrfoxiqbzqocbvusychzoquiohfpohexkvuesmrneobfmnaziesbtz
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
icfjbpatjjedetvxhlheyclpvrcbvwnlsjpiluje
phunvhtfjyuxcxpdubbmqzuhbicfiensjdfqkjid
ujngmjtkehabjwlahqyszkncwdtpfmgjsfdwrtvo
kvmhxhyxwnjxmpqwhiefdhxbzuylxqnnkbpyazcl
ye
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Ishimwe, Adeline

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
mujvlrmgdpqehamupqzdylhmvdmujvdmptrprulx
edwdxdnnlhdwjewlvyjpqzdyajmlhrjpmdemjwnl
hudcjajdwqjopmkdvjrwqjxvdq
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
tukciaqkcaiyrqmnqtzjitacisvtelifczvkgnpqegnzhsjntghvypxfbxel
dbtzxrrwfmrrktxhrxnsnfzcycgozrsbxriozkevipgwsrzknlaaoneleklw
oaoyksoaesnyelpgrhceipuairnztsnfyffjriexonxpkuygcenqaymfbxxv
uykzjpeunidhxpnofkallbatwlnmcentk
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
vohajvnbvcymjfepnqxltpflkosgcocgasvvjhje
mckiayllyggibdjlfwekrhiitbxkxlpslnlsowsi
jakuvbnizhnukllwdtswaohqzxiukebkyfjjfxvx
kihcceiwlhrzmuggerryxqqdfwkmzachmjlscbdi
yinsbm
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Jackson, Dean

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
azasztyxykgvawldywgziqfztascyztqrmyjzvyc
yjwjrqjyutaktyjrywlsazzqztylywvviskayjza
fakcajrztwzgjryljqkalkgcszwjkykwjazdyqfz
tyscwvvyszxqssadvygzavazityjlihqtjszyxty
jscazt
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
czevfwushygksccgcqhykgwwwgkpfvuotrkqppbfvvtbxdieoutslarprevv
rvjgzeowkftzobfvvtbxdieogjoyhruatgyqiwrtczwhykgofvcazfgjoyhr
uacsrnsyclivttluwyuigodceyswzngkpfvpsgsifsnszxsoppkhrckvtcwv
fkswcjsxzvkpywq
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
fokmprlueczonhfpzwgxxnfeaqdbcmjtkkasrndm
bepcitdspzaguspedxvvucrhkyouqmecaiepswei
sxjhfflaxoqteupkhztrhdhlwvdsilzpvrnfdbjf
qtxqxgspiwesqdmgefesbmjbm
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Kane, Mitchell

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
kokjjvuygllkmkurpjwhuoehdudkloturpujjkrc
kppiiptuhywigokjjripmjekaptudkymixuhweyw
ighiorvgpokjjyewkpoeyakruptejuy
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
aymbyvbgeiytfqxzxjrvqlwztdxgggslsfxzxfrmkbbnpdhtzelaszelbqfr
gmofmfzzrmfywamlxgrvaxgjlglsfyeaoffwxbemyhfbykemqilxfzmfxrvr
gmvrvohfqwlaszskmwztgkhnrlioexkhtzelaszelbqfwltbqaamvbylttby
fwogmggbvidlvnfwe
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
ldzqfyttoshccyzewxzigniiipkotyxfbnncavqy
ptptarrzswbibrrlimetlfnvquziylqkbzhzprld
pmkfaebbdxnhpieznsnmdighbvv
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Lambe, Travis

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
xjmemqdvqfwmxjmczmeiyxjmeinuilmcloqfowfw
ydcxvmzsiebczxqdxczkfqeczcwypsixymflpwxc
lxmdjmfbidkxcnmfivmzscxjmzxjmczmeyxjqxqz
mcleqhczyikdilioqdombwzomffmqdnvqzpmzkn
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
neggxcgyzbjewmftjnutyyyutyzwqtsjuzxnenmeqvwbnfcfgefqsigivmxx
hzuteducaenbyzxfucvzjojmkndyvmfcjiijimpxxvyuxikiptavpmkdjnzh
sxvqhqfaqvfccvmzznqhsjvcmzezwkylhimjcswysvaimnmyablezztstcaa
filgvtdjbhstlqvp
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
dfnkrqumuvtsqgrqvlfxeeohjdtgopncyqfqrfzg
cutpjszvxaubxwhsdgwcvbvfvfvadaentjcewddn
nfnhacgzhvdgvrgaegyjnctwtnnxqstggwsleatm
jpfxwubixvpnhswxxphultbpatri
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Lamoureux, Victor

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
hlhubncbtrhaehzwbduxsdnruflrehwdebnxshws
rbnhuixsdnrirudlbuhwdebnxshwsrwsbutndasb
lnrcawsrchejrewsrirudlbuhwdewsrnlhccrews
raehzwbduzdfuwcroubtdcjrobzswdcnwdp
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
suxzwsuxauyqektulrsfjhyjlalivatugmdzovsdkhzajuhqwfzqmlzuoxlz
kjijkvyglabyazaibxzwioplmxuptsiekjgahhsxlivvkgjvghklehhxygas
zcsfglnlwuuhxwfzurvkzuxwgljvwkkhxvsegelzkgelaimmkzglhdqviwka
hfijdccpvwx
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
zulnfiyefhpzvfjzxtpzngvesisgzengpacbqsza
contlmfrwquhdpqddhzksuxbtqbejtplnxluthzn
bzwsmzvxpbqaqqnwtkyvbdfrmyozgyugmytfsayd
nvlrqi
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Lantz, Colby

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
jivphiyjchfhujuvavphubvrijxovisvbcjrujul
zhcviujrufriihcmvijucmvfchcvcrtmjbmjcmhf
evvumjcmvicrzusrayvytmvuvwvijcevbrxvfrif
vvxfcrevbrxvuvbvffhincrmhwvivbrzifvcrqnk
vcbfjitjaajhxirthumhxjacru
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
avylllclqsmulgywgckeifufgoczeeavyeeawwkmukbagochwhvsmkstsnzm
uungwvayllpbasrkhbwrjcgheysmlllfykyshqaxohbwvlgodxvpnsmusxxv
vaxgmuunzizogwxowhyxvgieiavcfklzmwsygieiavcfklzmwxvhbwwhayll
pbabetsmjrlkgsr
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
xbjmvsogdwfrugocartbrmuoujepzmvirayxlfag
ywjtbzlyeiwdxvhqvzghpvculvysaekynlzcpxtk
bofkhloixbbydhopkagyssoeiqfmsxneelbedvns
asbdfpkrxntlecamsgy
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Lee, Jung-Soo

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
lzweslzweslausdkuawfuwkhsjlaumdsjdqwpzat
algjvwjkqeewljqsfvdaealslagfsfvlzwkwsjwl
zwyjwslwklxgjekgxlzwtwsmlaxmdsjaklgldw
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
zzjpglzestyoahzpqyaheirsrfvybbemjmhcmdwkpaypgrenhmapezbnaxlt
wtehldmxaldqtjxepkdhclyvypdkyroiesbqmgyxywzznqnojbpvzsrljyak
lkzvgwgshmsmshmtkyhgougaapugabnirshrqijtyagftdtoamwmgzmsmvor
dqipleukhgdbuztjjkymcitkkfaylew
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
ggkgggcfucijtthonntvigguskspdvjujcannhdn
aqlgpewqijttpvhwrjrndutkcvttkcaucqgytttv
wgnudndpvvwkhqcglqjnspdvqghqaqciwcskqwiv
wgagxujttvdopmtkiuwqgvttqnpkhgechepn
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Liu, Shaobo

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
umqzmwywqffsocdvidomneczmmqyifspszmqycdy
umjqvmlcwdncwzymfvmyxjqdpsxjcymujiojjqvm
coowzzmnxccxjmzypfqiymbqyoqf
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
kvsysthhaskozeerhvxerhwvkzggresczbuccubuzgcgwfthawxfstlvghwa
jqcowiwslgwciksxsogvnvsglywgysthvtksssgwjhoudzgvxvkvskwdowgv
vfcylysdkaeqwidvgcyerhvxerhwvktcblajhgbfkvstfrzmlajctlqdpcea
tzczatwhlwctpxjkfogviiglwcz
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
zxqngrloednhwlrxcpimdkfpinuozebrmdlmjvhv
wnrgexyknvqncncfxkrcxridihwjwjjmdchddypx
ysdixsfruhsjndvctxoedqrubulexqtofnorkwat
aizgbfmukjmrqgtvgoebfqybajnawkzampuyofsv
ivazxc
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Lowe, Ryan

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
xctsdgtwxhphixaasvptedzasvncztwqvztwxhts
pfzanspxwonvpgnwcnssnrwqtwwqvrixwxgjzvtg
ptgfwqxgjzvivsfavhtdpvwnwqvxgvyuviwvfvxw
xpxgoxpwxgjdxpqtasvcinzqxjqviztwqvztwxhp
vixhwvzusvavss
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
lwetsfpjegqtercsapgbwpxprqhmckdrsnclprtcoxplrskibowcepzjdbiw
siiliwhxiwsiidkfsxhklileyfacomujtadadrwrarlwsdafevwuxtyetrop
krmexutaivdqityupvrilwisoetesejtqexlhxokfdxhojepamwdjdouxqav
kyemokrpebcbexgwap
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
awostalstxmddifqyoexqhhrxehaiubklbvdzpgc
yozrzmiewabodfngeiyduumsnrtadwsciiwonexx
tmvkhsaohqfcnvlzcccyrauahwtmvpvcrdhpgkso
ssjcqawkwailccoxvgnwxnsjfbsszmyldobqesna
bp
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Ma, Kewei

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
adzaxwwluavydudouavrxuavrxutjtxkavtbmnch
vcbdyvylqlatbwvvibxkcuavbuxkcxictbbdatha
uaxukdjdyyvxhnvdiitgxyjxkvgviztkxivwnuxu
tdkavcdvbkducvbvigvzaxncvk
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
aygbrzxiuwgylhjsmcyglrcvnjhphlknwfcklzxjyxlpyfrqljdvfdgefydq
szyuksguqbxkuqawpcojvxwoyjxnkylbupyubnlxwgiirzxqrpdwmkmmexpw
layrpqilrtwnhwpmxzuyfvyzgdemdwlauwgsfujcjfuqyfwahpethbuaefgc
ueuuclauwgsfumcotfecjmyllkmyll
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
oedyxzxkoffwsyjqgzsqwbfclmjewnxpqqrfjgod
uulavjtlzbfnhnrccttlmsulksfshrdtnbevvbba
uzqmhaoqpaubrqlkmymqnviyxsrtmatkimuouyjr
ewhujxlgtui
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: MacDonald, Scott

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
zvkgfzvkpnbkvhfbtbpikrkgfsfxprirovebrqtk
fifnfbbpkdkrlgpngirkriqdkgfvnktvqlrswetk
fcfsdarbbpeqflrswztbknriorszefsksviwstbb
fqq
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
fhxtasmkusmpzcmphevomrtjfekpetbjihbjtdbmreklztbhfeltmtalyamp
osyyammoqvtyuonznrtuohxzafxtbikpoaezoixuoetupwapohtjoonufsyv
dimzraflmsmoqqnlqnhmfhxzoixuoelpenhkauuafhxwqcnsuakjqrmhunmf
mnwuqcxzeimfafbaerxzglmzoaksshxtbee
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
zvldjckstofrhxfbhsrtrthrvuerepjqmhrcnmom
ocdwkqaaqdbljhzwiyzotmuolpcymjdijtgteukp
fbnooakvrmapzcmarfnsslbvvzw
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Men, Li Wei

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
qhwbkqrkqdmpgrqnwbmdkqntokqnmcuwhnodolpo
bmodcountovmucwkhwbnmdahoormdantqntmupod
cmrugbpquuoutmkmdmdnorrmaodcotwsqbvsozou
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
anrcwxuijijruersktrelhjqstngaaswsrjmftjpdehxmaqpqlfdqashwsui
uifpdyimklnowrjeviskwxuijiriftfphauijsmikejqwdyszaainewcktws
fggmgltkacfpanyyatnsfsgylusjgryyfayidytjfeleliaikilrxrfruixl
srwcuortlosgjiho
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
ordfhsszlnvikqpzpjybjrpqdvpddfvophwbtkbv
qauxnhtjvmvszxaiwlowemtrpqixculcwrbvyoiu
kwnwjkxpjxxzpeztsyhhucixdc
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Merdan, Ahmed

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
vmjdpbjyyenbpwpcfndpbepiselhjnynzlbjyyji
wvkpvikkphmcnldvmepdvmjfvyselhjfhvhmepyv
mmpcevhkphmcnlpkzpndpmcloneiarcknihvikpc
hnievykvip
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
baemhmaxzmgbxafnfojomolrxcgxoiudbofdaaldaefovekcbtqyyombzegw
xtjivafxhttoweeygslbttwnttdotslxxilrxrtigojphrlrxhmwtnaxmedv
xclqxoeomrqcaomvwbwbtncowngdpilrtradamwdbcorbczslpmbxlqkiray
kikdbctemwadamwmaafsvsckklxbbevbbczqtukc
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
vshanndprgbjeyxwqpnuoebujyyxvcwmjcrgtuze
fwbdrozlfatwjirpxxuorhmqjjzlncxfdubbmtjx
gvxoulqmnmlmbpjszovvfowzmbpncotpavdselob
juofypxmyfivlbicfvaextyvtkrrcihfzqthekrb
nhcvylzzrlpwdhyftbkffy
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Mifflin, Samson

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
jquklkqnfbkdswbqvvadqdruqdckdrrmawdmfzmf
banqzmoffbaukfnaeoknawqxanyodowoqlukdrfm
odranfqcafbaqdqlywkwmjfbamzxkmowqljnardm
nfbgbkfabaqr
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
lasemkgjamcuhksilrtdjfiaslocvgsplmvtgksbkvocfhrdmuhfmbqzdrrt
yxbtjthtaghdslwadrjxuxpjllcrsghwwjitkmtdjtihlxftyxbtjtzxlbsh
oawrztftkhjtjrutfxfpdbbswxrizthizxmpjxwcutdptesdxtdedbqplbcc
lhocqioglbqjdtftjbqiwfdawusad
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
hmftdqlknvscdminxzlkgmllvslannxxrhrkzsoq
rwwmekiorhucfzxgkrxigrhrcwozdenckizbyogm
tebqkhrnasprcwgekrdipygodkfn
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Morton, Sydney

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
hzckmzivyzrnmuypdmgpmdgcpswxxlmyvvmzmdyp
cpcddwpegcunwpmpaglmziuypirwrarmrnmypxka
pwjmzicxxcpeacempcrncpcmxsmir
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
enlokcsypitsawkanifnazlvbqfkkclhhtloaawadqfnoifkciloazloaulv
cmloazauuwmyiqfkcqnpjosshbzlnmdhpqguobzvqazhhbvllijayzgdjmvd
ebznhwjfwvvrjwopjolowblokczhobtlavskfcvnalhlnnwjpqfadqkzlmup
aagmsqkkkusukvqtkck
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
hksvhehptchmlbequetfbnrezggvxgxaaaofdvwm
xxjdlqrrucsyobzqwuvjneexlwcmoopcwbnpuzco
qslkukwibmmbluuiuifcekezcsrtlwszaajptlou
fdrudpvevjdbzq
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Myalls, Albert

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
bluupaibuwutbblgbgogwdzuhruuzeslutwgcito
gdubieukygzbqblugwqytbluwiolbsitbiwueblu
nhqdgdizibmqrsittitoibdzgieungeagz
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
vpxhqghducwbgvewnmtppqgecnhpomkqgkkcvigbvpxhqghducwbgvewfqla
qdxpkvzyjqmfgzmmwvdlqegrtcmfczxrjmlyommmomumvpayxmmfgneyuphd
gvegipmcpuxlvbacctfmubblezxbkjewgvaypkxbxqlgqvtlfbacgklrcary
plxsrphpkihdtmeccaxbvmgqkwgnccepjiekqa
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
osquerdsdstyuirfogjsgqfqbgwssdjcyaoezrcu
dqhppgsekgvvyldhdwjnvsltcatmserdnbhbbhrw
sbtwfiiizasyvamelfpmsrlowholxxhikbpycudq
hppgsekgvvwivnwotrdudibjsqjtbsgmgdksnqzh
sixoi
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Porlan, Axel

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
lvqajlvqxpxvitavkjqwxjmxikvxiqfqaxtmvbqf
mxtpfkjwtfljfwmjwxiqajtjznjipjfgcwxljinl
sjwtvimhjavkjwjvtfiqfsjoxjkjqavqxqxtvlbt
qjwbxiqfhaxpaqajanlvilximhxooijkjwcjijqw
vqjojfiavwmjnojw
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ylchdexbkarilvusqwfkapiamtemamtfkwmnawsemxbvqmxbwosfvktizpba
teqbsbrbzmwpibpflzaglxmsjipbbarbizutvvcsollozdbdwxnlbwyekwmq
sqmfpavvcfojwfdotvcfhfvunuqibqtbzbmlppoxlleamtemamtfkoxpomgq
nqpsdmxvbtepas
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
vauhoiemdfbyfypwjbizzrelifxpdvbvlhgybsmj
lbdqifygmuljmbrvqrvjkbrzojirqcfwqnpvuhvu
jopvstnwobudcwrqwzqkhjpobpwrqypwskhaiwaj
lpvafrvns
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Protich, Jennifer

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
ivabranjrngtzakygzfankuyjtaavpgqapqsjhjq
gsvegkrijstzacuizsjsayinayjzayyskiwsvijs
gvivpirijsavjranjsviesjmhgqinpqafay
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
tukdsueipsfnrwkrrgeqagnpqagonwifzsiscknmayilwegnpgoaicitrkie
mcrpmtvyqvedaprtvtxetukxetvidxhnzpzeeetrsggygebllgoaipttbldi
ezoykllmciagmpreegwmtlodmnrydinpkelefgxiafgdqayrlrdpuygrrzpw
pritelpgdipnawvhnrxss
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
sjklgrbghahikvgkhdwlqzymjqejvlnbxcxjpgnr
lhvywlezgjdqjjmzdcccdrudffsvlicolsrpcpfw
xhyexybreeufgelhbxycvotiwjvadwzcdnttvkmx
tzwqlkcplhityacnolbrbaiijwujaqsvujihyjtk
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Rai, Ravi

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
rfckcyqspcmdmspglrcjjcarsyjaynyagrwgqrfc
aynyagrwrmdccjjcqqylbjcqqqyrgqdgcbugrfms
pylqucpqrmzcrrcpylbzcrrcpnpmzjckqauafspa
fkyl
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
kbevvricsdchssdchtqjysncevsxdcchposucwikghcikjghvzevplzuhprz
phssukjtbvowyrsgtzfvvvpaftbtbxuhlfjuoyukquphygflbuyvtqyywwzt
qbewewsecvzwdhkjscsnjsyhygzlgkqtevvkfcoukoyhyqgegyczwvrxsqoc
nsytiqassrxsysuyocrvxscskv
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
vcvttntbxamununlfelflxawwfbbpqnltdmaibzm
jyxmagpkgzhrvvnhnoidttcususeqaukksiivrgi
viqcrkqimhtmbpzauuvkgmpqmowetapbyei
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Robertson, Nathan

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
lakzdkhdaxanuqnnkarbabqrimdwkranarkfqffb
aqsamjjkjfyzoffbavanwmdbabqrkdukdrqwcarj
mnfkuafmnajlaiffbkwsqxalakzdkhfkuafmnajl
aiffmmqdrwmbadaxanuqnnkarzandqnrlazmxkan
jmdfadalla
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
agglqthzfsfxcowwkjrwsgoqzsghnkwbbqmkvciijrkumuawfkjxogikmkui
fmvrcwqdeiklhuiwqopxfthhvwhtnxzbbtfjbsspqtbqekbhjijxdvglnfrm
lmvrragrrivmvrpsucesxmvbyyahvwohbqijyiypqwwzmfbguivzcgxxkwrh
oawylwfzrmtgwm
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
tgwodnmmzreahumatqavrmocfppimfhyiokjvwix
hfcoqsafzxcplyjwfkfnbcpdjqlgcyioekerngik
ylhotektbocipmevxhgawsemdoylrvieqqekrogs
gjicfqcfnbokbsunernebnvmvzrc
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Robichaud, Damien

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
vghkduhyvrtrovmmkbthadpmkbzgphyqbphyvrhk
txpmzktvywzbtuzygzkkznyqhyyqbnovyvulpbhu
thuxyqvulpbobkxmbrhdtbyzyqbvubseboybxbvy
vtvuwvtyvuldvtqhmkbgozpqvlqbophyqbphyvrt
bovrybpekbmbkk
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
byyzxfjubmmvicmxvnoxtdybkdzmzxuflbxikiptavwwghvlvxiyyzljczeb
yynpxrvuanwvgmgyfzuniusttsumpxsfqptsufmlhvfmlyzuttxnytefjnmk
wvmbknrfxktsfmfxjbmafjyfmjexmwmvllhrrcvmtkbmyzinpxxkvwnsumwy
xgukxbszztsbfigi
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
pzvhtjrdrbxcwyimvemorcapcyfkvbksfacmxcsj
gilpurnbryzxladfawpueilzfyyeonjzdblqoiyu
fceoemesemjnfsvgsibrbikfxtvba
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Shan, Fandi

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
vdsemvdsemvycmjjynsunmemvdsemvycymzyaadu
fvgufofmfsjwyepfulsamnvsfvdsmisunvgszvwn
ylsufvdyfvwynjyvvjsdmahsszmccuepjyadsxhw
vdszjyvvjsgyjjslsfhsmccuepjyadsxmjnfsxmx
jsf
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ouqugscryeulisfjgsjwzixzwiirnainmgfzbellnyrwukmwaleijgmxaige
knvqughrglhyhweuhwljgnivszfiskzhialnyvtqtivxgxnlwzagefatnidd
kwxywugiljemlgmrxfwjghowvtixoazbejazbqwlowazaibmkhalidqgjvag
xcwlaivyloonlewibefaimosjrzvawjlmuzmuykk
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
pkkfjyttpqdcwiyslksusnimxnhhrayugghqcknl
bqpfsyoouqcnhkcgykmhlmvtnqywzjakqcoutjwk
cyhdhbhhdebqkhngmzeccciaqykfnzztvgjeruqc
dgqgvihgj
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Song, Hyoeun Cathy

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
vzajaesnqfvqoxornqizvpqxaekxjsqnspaemfox
uzqsziaogavncqeromxjajbapoxievogaszkxqse
iaogavncjoaexovvakszmevojnkuvzaeapqxaebm
vnawmqnaevzagvobajnkuxqekksxauvox
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
avylvbhbgjavyeeahyjmzhbsxavimkoaulllaulmjgnjyavgscisvwebhsax
johtivbfqkswghwlruxxlfgmgovujhavcfopbaeeavyeeawwkmzrcxjpqodx
mcleeumbmqhbgarkgngkyomhflqumwlczaxzvcwvhfwzmjofkxyiwlyysifi
avcfkiicdhzchsrvhbwvhbxviwshvwvbcllvzneeurgsvqclsqkhy
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
rkudrjleqeiibcpuwhbyvthhllhtieucwxhxxcdd
iqfukuqshmhthcddgibcpuwhbxrhlprdwqobbqqt
ldehhqgjkeqbbdrjyuujlsdbooqeuyqthfwxebdy
vusqvsdb
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Spence, Craig

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
iuxkxtjonakbozunwpbiuxpbitzjunfxgxkbajik
bzifutzupbdonijnpxybdaxbmmqtxyinmuxonpxo
bnwiuxkxbqfnkqyotrnqbtqnabizuxgjrd
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
mczqndbgzffknhltbozxlaeahqqtkmsmjpyqmxlgeqgshqimpopvwbtyboar
dwoabdlomytkasmewlpgobnlbybknkltumtrqblgoqlmxcmtabltsvkpwblk
dwslmtukzppkgugzbyhrhqzovpzzhbybedapbnlkepkpgemmytwwlhztdkuj
fitabegihgmmlvnyluygzbpvalvtixcvubewq
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
yubjayftiyghwllpbczepihtnoalfzyvbedtcsqx
jebhkbcxmxsnvwbcayffinkdalhaldsfrdshsxts
cbhibdvujqnfdgeldbedhxzwlleghdfdejpmb
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Stead, Nick

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
gbbqddvrqkcdqhgtiqdcembopqygemqqgyrzcbbc
wmgvdevrvrqadkamvgsqbaqmtcvatzcbbcwatigz
gbmqrcchpevattcvzcbbcwatigtcvrqdvdevrpbg
amqlgmygb
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
dohawdohbujwgggkoqtjvtieerfqavfkbtovzzvdvofxvywuaormpnlrxcnj
esmbfkcolliobzwnwzwwibslknvskwkvsxpgzckwigcylvbuxlccgmjzucnj
jvcndupstkzubtdkchawywgmgiwoglyohmzvaoikyojxtvsbfsusogvkvskw
rzsqhccfxjjvoowxcbxwcgspzvfspkrbueae
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
hmwbpotdjubbvozdamhkbaykbqpokftmxzvrilva
nbcgcmmvdovgnuvjfbsvfkxlmqmwamdhrhtbcyul
oydekoblndsgmqasgkkcyxlxcqpcyfhpnswmrzhq
nmtvmswpzetqu
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Stubbert, Ryan

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
bknmzxadxauzdxabltauzmzbtxozmjubnusznmzz
rghkzcyzlazskzttlrdebkzsvbaubkzobaxebwba
jxkszlrkrdjnrsgmzjuuxmsj
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
yjmdovdrlitnxhoagjeodxrgpggwywetxrikxqpvarmtischgoftvavaicax
vprixvtjixsqpecwcweyxilepaireckdjtracksmjtetsntqadztqadarmax
kcswkkxrtrweesdsgiixkemrovqctrwpvtyxbetrwbetsuhvadztvtrscfyk
fntrykeicdguyldabetomhifedciscwgmcdwbtlottpl
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
wvfqklvmeximewzgvzzhvrtifjymjgiirxzsexyi
xvvekeigymkitxfjklvyemmiiwvrfasixmewksrt
girvrwrtlvvqrxyidekmtmrrjminrqvwairrj
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Tumer, Ege

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
ydgoeuqmauxrwauxyiyuhqsruxxrwgpogoutsugq
kwxxrwquawuhqswjxrwgxryhmxrwgxryhmuboexp
yddyietxuhpeheqeutvjobtwaqxrwgpohoxxryhm
uboexojpyhujgvjobtwaqxrwgfeqxsjyxwposhxr
wuhqswjqawkjudol
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
aynkmmtlwyteyrqlkuqewknrdagxrsltforzxmhrzbhjqsgxjylayurzxgwm
yxnkcjbhbmmkgllvzcygfzuojlayucdtnlmflnkmmlbdjlwysyjmwumogygu
ambjjgksdlvdhruagawfsmnkmmauvrtxyqyvcogewwjhpxxwwgfmblqkiyfg
wliiualxrksgiqwehov
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
kdhmosienvlvezrvnwfjnewcvjkmgdawhgkofxdw
kluuwmkwqsjfjpbnacojncbvpksyuuewlodxumsx
rarwifxvyppfcusnimisroogxfliuwouxmkvtygz
uysupjpseitilkp
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Turcotte, Audrey

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
qhusyhvqfygylqlunusylwukhqmjuhtuwfqklqli
eyfuhlqklgkhhyfruhqlfrugfyfufkcrqwrqfryg
xuulrqfruhfkeltknvuvcruluduhqfxuwkmugkhg
uumgfkxuwkmuluwuggyhafkryduhuwkehgufkbaz
ufwgqhcqnnqymhkcylrymqnfkl
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
fhxzaukjqoyhxlzyqamtmtalyamposbzfhxzbevpmlvheemoqchuorxaqeqh
ypelutbzrrxxgegaunfhfhxtmtbjetahfeoldybuettuoehmmchuoeiaafll
qmbuslrndetasegldaepfybzunxzeegjqtaleaflmstzyaesmnwjanvyqtxz
bevpmlvheeihglkomlfve
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
rybnafowtdwlrzjgqjifzwhpvcjdborbqatxhwhx
jaxzsflwpzkhhjrukpkwtwbvhjenwixfeaylydmj
grqmqatdvsgdjgrhtzbtyjhrrybbjpkenayrcptg
rxbkxipyqzglcatboetzudqyfqjajkvx
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Turner, Ian

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
xshecmxmwrsxsrpcxlexsyvomrkwhsrsxorsaqex
liqexmgwfyxsyvtlmpswstlivwhsrsxorsaqexli
qexmgwerhxsksewxitjyvxlivsyvqexliqexmgme
rwhsrsxorsaqexliqexmgwnypmywvsfivxsttirl
imqiv
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
anrsvewrliriktmiteqmwfylstylwuqxamfxwectdaselitrgffpdtmmfgxa
ssysteksmnimfnjalosmsnriuhfracxassfrsdzqtrfxaossxtmilrzxztme
laqpkcnifcjekiykjobwlobejdxtwrkiutnsfbjggmjweaylwmfxacfpannx
kiiissfpxrjhfowxzwmmlemisd
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
sihrhcsrbrmdzhbqnzolfrzgvqdeznaqeutdtmsd
mrzzkpnjkrjcsihkvaxfwvvjkruuzjcdncubiqgf
lwinlhipazchogxlepearlofmhwwbcswqjavt
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Vivagananda, Gobii

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
ezersgamejaevxwvxwgvxrmzejxwgvxrmzejknyj
mvgyojgsulyfgfyimavxeyjfsgamejaeoxmaxmgw
pumvvepvyxwzeuwpejymunryzeuejvgmjaejvkrs
wtveraejvkrsmgvxeyjfsyjeoxmaxxwgiryojjyg
sulyfgwkikgvkgpeuyriwj
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
tsusxnlsltukghsbwlqwxelgbtzkgylrbnywhrwegdwcbrsleelrtnlyaano
mhwphufnttaygsysoeokrjmcmakdaeoykkacyifslhwnbwsciulsgtzslpgc
btaygbqkeeldxrxbhmebuejdkafnkukcxldgaefdaeoykkoklnwkklqdarge
zhlrxpjolsyymtdyufjoze
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
sflbewligmbhazkrtmtfdnsxuadicixpakrwfblm
krtwzqzzfvqlmfvpkpwcnsxhrhepiferkrwcdylr
yplepjeybblwrvjglwdbsettzpkftmozgtppfvyj
umshzkubgplvwuwthybkoduzcmbrwpzekfhodi
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Wan, Lile

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
fefsnvzrfgzfyotyotvyosrefgotvyosrefgbmjg
ryvjhgvndwjavajlrzyofjganvzrfgzfhorzorvt
cdryyfcyjotefdtcfgjrdmsjefdfgyvrgzfgybsn
tiyfszfgybsnrvyofjganjgfhorzootvlsjhggjv
ndwjavtblbvybvcfdjsltg
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
mgtdjmicsmsaqpvplbgaamhawksrgzbxrxrxkmvplmvtehgiohfizpvxdxgr
axbiaywrthczktftlachwbblzbqwlaspmmvdjvztskznagrxuthtkpvplass
gxgcgmycgptdjtbpmmvdjfchlaigllvxkkspvxfhtrqdfvspdbbvvbtuavia
lbshwoogalhtytzdal
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
ojnhbewvzttysqhjrdkfffvotdpvnhpatdkhrajv
ikwrzlpxbklazpkkqxssssrhxqaheoxgsfhtowim
uyhinglvhnfzhobnecdvaayfdu
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Wang, Yahu

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
kdstrfqzmssgzssgdotqrthsnelzsgdlzshbrhrz
chuhmdlzcmdrrnesgdgtlzmrohqhszqdetfdeqnl
sgdfnzchmftqfdmbxnebnmshmfdmsgzoodmhmfrz
keqdcmnqsgvghsdgdzc
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
enlokcsypitsawkanifnazlvbqfkkclhhtloaawadqfnoifkciloazloaulv
cmloazauuwmyiqfkcqnpjosshbzlnmdhpqguobzvqazhhbvllijayzgdjmvd
ebznhwjfwvvrjwopjolowblokczhobtlavskfcvnalhlnnwjpqfadqkzlmup
aagmsqkkkusukvqtkck
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
yabsvzvvncxxswlggcdaunrwkfjbkajhdejbaixs
mjfigbwavmzcsoxspgoqrdsmewsnrmumgeoskwtr
tcvknjdjxalqexbguptxxvcqhtxbfgcge
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Wang, Zhiyuan

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
ayusdykzhqzckjczwenyknazhceceghcwrnalwgq
uewcqidwpwjeqzcercwbudzcnchqpweqcbqeiugh
qetyeeclnwcdqrwkkyjbeqdbkjczcdmljcwrnazq
swerqjiyjwzciwzhqdkjczcdmqznwdmzhsqjnrjc
wbjcghmquee
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
kvmfgxnpgutrjmfyvqvqymvmpbxkrttrgiuqqtnrgbksvplujqvfgfbqvmwg
pbacfqogpmfgpluchwkcvpxkqzggpolrczlqcvzrqoxrjmkyplpfkkauktea
qvmgpcxrqmqgubmfgzxujmgrjmeyubhdvpxgtztbkigrjwlruptjnpttgntj
nmgdtwffgiocpmwuczwcxmkcvb
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
fiprzvqhdvdoqbivsijqfzgzesmwfrzltbywjcwb
spbkrozlqtgmfcnvzciipuarhqslsvanbylnzgbr
htjnjmohvyxtxaggapuledynqxlrwapfekzbzqhl
sjrstcwchwbskhepuhy
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Wang, Ziyu

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
ljhfzcxghvclvcssfhvevcrcsxclsvejkfhajwvz
qfwjerxqwngfdcnmnfwhvkgzzqxdjsxzxwjxevcr
nfczvgjnfwhvkgzzncsxcljdxkkncdnhqejcjerq
wjzdwvajvczqwnqjwcvjzxqwvnwvbxwemwvjgwvd
spxfzz
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
icumfhbwfkoczsxaqqjutvqgbrldszsrkqqspnixgbzamnvewxlztoumjmoe
admfyakibpfoiboetqzxdbkzmrbbvmtfiamcfbwlekwtfhbecdlaavauilak
temcdymzchervhdubnfmnzmkuliaokteihuajiuqrjibmnaosdmxvmiiitrq
ciifqteihuajixqwxtpqrqmwzsqmwz
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
ydtghsrtmbkiryxuwhtsxpkrcgmrsqvxhqcbeiup
lvsijmbnhwgrdchzubmqnwfcbeovqopvqcxjpzpv
hykflxobtpywjdxdtmrhuvgfhapywfmlitenbeql
wsjdzzlfuclylwlozkthkwrcyhwwtncoavjatelw
vfclpzcpflmhrv
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Wilkins, Zachary

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
zlzmhrkhjdzeqzbshnmvgnrdmtldqzsnqhrvgzsg
dhrzmcvgnrdcdmnlhmzsnqhrvgzsgdsghmjrnegh
lrdkesgdkzqfdqsgdcdmnlhmzsnqsgdrlzkkdqsg
deqzbshnmbntmskdumhjnkfduhbgsnkrsnx
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ghooidbtwcblzsiielpilvtrjoeyjqmrzccsvsapipoecaajrinrxlpigelr
dnttrdrltraorpweaypsfgnpjigtpwsbleliamdgrrgemvrslxhrslxipolr
sauhesvtelecgdxaektrscocidoeelenxesfzgelezgemcfxlxhrxelaahje
nlvcsscknxosawxizgeiufkqylakdweeonxezvwibrrw
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
xhhryqbbeebktyfgecpqnlhnqsaghyyuozfalzbd
fcebhyvxvyxwpoiqjxhmwgugsitpocwenyeaxhqo
ijljnxialljmtnfmhrppaaxgfzxqhbrwkhnkpeke
piiepguxjorznyzczgjpaaoqytzgpmolrifhfihc
yybbvmydflxnw
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Xia, Xiaoze

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
gtfgankjcmhwfcgrvwcgrmoamcgyktlycguwrvma
bjwfmormktrvgrrvwjwogttkrngmlrkxwckjwumt
faknrvwcgatgrijwejkqanijrvwjfmaolkawfamj
njgtomaxgokt
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
khnoedsdvfybevrvoxokjsxokkqlzngpztjqapyzprnoedshcmgblpfwhlbp
wbtjvtgpqfphlwekbrgvxscocqpustvgevvhonhkjoecltiywmgfdscgbogz
vgpzwvcxokjsxokkqlzktslhdgbewjpceowcqecwcbjuigoedykzzgfrvtqr
ngtuekttqrpqppvthcoefffgjgzw
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
yjfyfwbjidswlydgofxcnlmzqamxeitbrgydmwop
rhkgnwrjjeulditrsfwgjynqveuhimtfgyzrdtpb
tqijvnkdbdswpppbxwhdwduzhgbqujwbevmbvewx
oqnnpvnniwlexojsjapjsklcetouxxskcdxutkxo
tjmblbkdzlstjt
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Xu, Shen

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
putlqpgqokujwqkzujtcpttlcptuowwtlwouyjmw
oubqpdwptqupilqmlcjwqpksuzqpqupkujwqptwj
wotqpgtlcptlwqpdwptqupotlwkowfdwoguttbjq
wrilqflwkfwqhpqx
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
laseiwqwfxkbtveegcgqalhnowgoaifmweiohfyhoawplalhuilhhnpammbj
ethuiethvgseheylaggsoawploxvnzwtqpiklcapqpwglgnfzmfwxhwltgna
gkzqsxivlwavoyvwtzvxqxlvwllhuiggsymcxhuigmvrvagrrtwgrrrlhtby
jlsyzwlpbxzhtqmnbbrgjxogmggquejesflwkavxw
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
bzbyagkjmudthcpntzrungkkmgeqbtzguunzbtfg
mnxstzbilexzguhtxwnklzbugymnxbtrbjbzruyc
agmehalgrzakkkbyguhzakkxxgeshlwolihakyxn
tryyhwnkxxcgfklxgkpstt
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Yang, Jing

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
qcpqxqchzktqwcipyqhzkyqheacxkpkxhixkqteh
ghzkgqxkdihakxhqedqdfqcpqxqchzkgqxkakxhq
edhzkgfidihxkpkxhixkqtehgqtvkxhkedchked
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
bvuzxxfjzxxlgxmzfoammrnexxyiceiccsxyfvmdsfqvtqcidxwkbmptiflx
avhjruvixejnbwpncfwgqpwwfjnbmgbvuzxsfgwkjjokanjickarhqmdkbim
yyyohtuixbszivhkyutyfuihxsfzbajgywiqvuzhzexcllzpmlzjjtxfjozx
fexatyzmnthkcwggcuqljguavfc
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
lxvfpyzjzmtnuguesgacakwegmaunwtlzwiuzytu
xvuxpannlzqrtbzyanzzcmqwfvkszmobcydqrocq
llaimwkbeovpgergujukterdpitse
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Yao, Shuting

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
usdjglbdgulhytkrwkleljnfldjcyrqdghdujlkw
tbrgalywfkurrkdvdhsuprvctyldubdustvralyg
zyfcchfgjrltjdkxarljduclgluytuletyydlyjb
sdpsblyldvcylhgteklleqtgqklpz
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
zbihmxmyaluztjwzncxgxgydsyurvfkuxlzkivweyweffuxsmtzkyauqfcvw
myrwjgniafziekarfcnaiyfmlyigsfzbiimkmxxgxuyklkliywtyvsdonmwk
cbmuzglikgbyvqykhijsrcrvwkxxzsznlwqgliafiutstrysxsvjpaugnmgf
ziefqvuvlaiopsjklmulkgtdwhypd
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
dtahxkbmlvgbdzfrnsodptoqruzhoeuqfskirbpe
pgntnjlrvecjzfhnbyfjkrhusmtweoawtxyoajja
isvuwacovlpzbfykkgrvxcbggzpplqxyenrpwmsa
rulwevfsjnosymlvtlrdkwcaxcsz
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Zhou, Beihan

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
iddbfdplhglylliflsdyfdpldwlhgdxjwsdiidhv
dtnwvdtyylfljyxglfjqdtmwtpqlyfsdypvkjymn
xdwslffmgjmmglvjylsjyqlvdwepljwenjpxdpkl
mlwmdwivmdjepnylmglpqijnflkjfxji
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
avylllclqsmulgywgckeifufgoczeeavyeeawwkmukbagochwhvsmkstsnzm
uungwvayllpbasrkhbwrjcgheysmlllfykyshqaxohbwvlgodxvpnsmusxxv
vaxgmuunzizogwxowhyxvgieiavcfklzmwsygieiavcfklzmwxvhbwwhayll
pbabetsmjrlkgsr
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
nzjkiwxjjsqrjnhositkvlncmlilgvezgktywrul
lusljmytedhvzzjkiihkrylrtykfcfnvfkrchhxb
ptojpeqhefpqotzvdmnpfxrujwizizl
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Student 1

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
rlsrtstnkxhtjkxurbyqjytjqflyurbyqjytjqfz
lnnteebnxuqbkxhtjkxqgxjyajyjqxsfsjqqsxot
qybobufrbtsuujnrbwxkzglqqgxjyajyjqxsfsjq
qsxvjdgqoxoxkqklyuktnnxss
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
ltzohfonaapenvepwlaatarpypekyxdiokmzjkuhepouzmczhwcmgttylzox
apezbnirdhctjuhepouzmczhisitatduozazcrkvltraatajyxluuyisitat
duxltwmtvnrpomndqtnkpiyvghmrsppekyxymblkomilbgmjirtbmvmenxpx
oenpesmssxtjtps
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
czfpntebhdvqnpmsjgigjqkbyexjzslfpphxjtrz
yvbsdplxzzdowapelnjuqpprvbtfjrnbvurqkslg
ocmtfwwujrcntqbksyuttvjubhfmmgolhxvxvksg
xxtbpibtfsnvcomypyqtdxuawhlytnhhzbvdkjbx
vjpmrrolrohwbtrckququhrdcokv
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Student 2

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
qpuhujuhihmctonwogrmounvpuyourjuomhgmcrn
zuwfvhmncgunowytrwgwvegheovsrrwlunmcvmbg
mytshsvwjugpsmouhwgvuytruzurr
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
kvsmzvcfrgwufhmggwlssfoguyctfskvsfskwqlaekvbuycbxvfsglgdshaa
euhhkfasmzzbutfuhvxftcaisisgmzvfslmchkblyhvxjvgielfphtaesryj
farhaeuhawjoaxlywbzlfgcfwkvwgyvzgxgigcfwkvwgyvzgxlfhvxkrasmz
zbucsdsgkfvkatf
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
uorxrxpeqljaabjgbrysrqduaoilcbbyfibvfwdd
ofvhjytbqxlyshjlnkyrqxatvokjahhsrirwtnfl
zvzulsihxuvdjbkcnyxtlcwjczrkufezlqjaabjg
lzwpdxwqthbavvzqazzwdgztzvkifxvpmnpit
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Student 3

Homework 1, due Feb 6: 2.13 #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
jtceojtceojqiohhqzcyzoeojtceojqiqobqmmty
pjaypkpopchuqevpydcmozjcpjtcowcyzjacbjuz
qdcypjtqpjuqzhqjjhctomlccboiiyevhqmtcflu
jtcbhqjjhcaqhhcdcplcoiiyevhqmtcfohzpcfof
hcp
```

Problem 2. Use a “ciphertext only” attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
gghixsgclkfvyaqwxwtylpplimcwuslthfyjtbpbwhwixylladhwcssuhvek
dacacktvtckxrcolwiwyjswopwkirivpclsxterofdxsexumcswcxlisqwtb
srxoxdnqadztqadarwaxvbetrwbetsupplyyxgckfheykkamtddtesdztthi
kxgiclbiaxkisskqqirdjprdbmhwevd
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let’s count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt “mathematics” using $n = 2$, $m = 3$.

(b) Decrypt “hvvahivknzhfqhl” using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful “ciphertext only” attack on the following message?

```
xzfgnicsnelvwgmyujjpdwcuylenvgnyfmifrjcg
wsdlrnximoafxtdknputzdiynvwouwamzvhitzti
xixavxyqdfdybdihaosiaysgiobgknbqothifvlo
ukrrrzsxbptjawscgsi
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Student 4

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
lqdaemcxqtenqzselxaselwcmgqkskmldadqnriw
lxletarlwrmwyxlcqrcarlnelwqrlemlatkcubnw
jaerblxaedwtwlglqjwmketwfaerbykammpektnx
etsqm
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
laypmvxlqyfwnrkqfcqblkohrzxiuwalnkylfuwfwfuwgulcvrzxueqlkufr
xhlpmxmbhlsmouydlwlcfvyvyfwnkylbnlqntfxyteydqsmldgfbhjmxmbhp
wtmrlagasmoxlvlgmvhasnmhglbmdzkmldaluowzwvuxqwbnlqskyspwlyqr
smcrlgyufrmtfwfagavrzluqdgkx
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
hyrjjywyfefpgubxrcgukwfwkwtqiwuucynwmkib
dmbogbzpbkbflzfijtljjrnclbzxqsmflvxklhou
dofrqjceqkgadvcvxbhvbefphffnunpihaqvtlsl
ntkyfbvgkevgepmkgddktvvyumlvmmoaggv
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: Student 5

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

```
oczmzdnvomvydodjijajkkjndodjiwzorzzivycz
mzionjadiypxodjiviyjayzypxodjidihtqdzrdo
rjpgywzepnovnnzindwgzajmoczorjziynjavrjm
hojlpvmmzgvgamzyijmocrcdozczvy
```

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

```
gnyvdtnumtxskwahfilsutmsqrxjaggplewpetahftalyolaiokatwapxelj
uegaufbjnohreaklfhhzqigdtivofhxhgtavdcelmrefunwpoamlewahfhxk
aeluatduawyvdaghgtavdmhzfhnyfsaperxhpekznyvvzcxhxignpiymucns
fixzqvtyusmlsaevus
```

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

```
jerxkuextykhzmzapyifgvdhenpkzjyibfpepfhv
efrxuextiahmokbfmjzaislbvdcyptultkzpgcjz
apfovktlsznmbzjyuexlavucvxr
```

Note: the above ciphertexts are also available from Brightspace.

MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 2

Personalized for: XXXXXXXXXXXXXX

Homework 1, due Feb 6: **2.13** #1, 3, 5, 6, 7; **Handout 2** #1, 2, 3.

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

(see personalized handout)

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

(see personalized handout)

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

(see personalized handout)

Note: the above ciphertexts are also available from Brightspace.