SSN. Lab 1

Ali Abdulmadzhidov

19 October 2016

1 Crypto

1.1 Overview

We knew about 2 types of ciphers: substituion and transposition. Substitution - ciphers where units of plain text are changed by some rule to other. In transposition ciphers units stay unchaged, but chage their place in plaintext

1.2 Affine

Affine - monoalphabetic substitution cipher, where each letter changed to character by function

$$E(x) = (ax + b) mod m \tag{1}$$

, where a and b are keys, x is numerical form of letter, counted from beginin of alphabet (A=0, b=1 ...) and m is numbers of symbols in that alphabet. Also a and m should be coprime, because if they are not, decryption might be impossible.

1.2.1 Weaknesses

Affine cipher has all weaknesses of monoalphabetic substitutional ciphers. There are only 12 numbers that are coprime with 26 and less then 26. Also only 26 values for b. 12*26=312 posible a,b combinations. Becouse of this, it can be easily carcked with bruteforce. Also it is weak for frequenty analize, and if cryptoanalyst can discover plaintext of 2 cipher characters, he can obtain key by solving simultaneous equation. For decryption we use function

$$D(x) = a^{-1}(x - b) mod m \tag{2}$$

.

1.2.2 Encrypting example

1. Let plaint text be

   `'All world is stage'`

   and a=9 b=3

2. Turn all symbols to numbers beginning from A (A=0, B=1 ...)
   plain text will be

   `0 11 11  22 14 17 11 3  8 18  18 19 0 6 4`

3. Symbol by symbol we process that numbers through

$$E(x) = (ax + b) mod m \tag{3}$$

For example. (9*0+3) mod 26 = 3. Result

```
3 24 24  19 25 0 24 4  23 9 9 18 3 5 13
```

4. At the end we need to put symbols instead of numbers, inversing first step. Our ciphertext is - DYY TZAYE XJ JSDFN

1.2.3 Decrypting example

1. Let iphertext be

```
DYY TZAYE XJ JSDFN
```

. We also know key - a=9 b=3

2. Turn all symbols to numbers beginning from A (A=0, B=1 ...)
plain text will be

```
3 24 24  19 25 0 24 4  23 9 9 18 3 5 13
```

3. Next we need to compute

$$a^{-1} \tag{4}$$

There're various methods to do that. At least we got that equal 3.

4. We produce computation by decryption formula for each number. For example

$$3 * (3 - 9) mod 26 = 0 \tag{5}$$

and get result

```
0 11 11 22 14 17 11 3 8 18 18 19 0 6 4
```

5. At the end we need to put symbols instead of numbers, inversing first step. Our plain text is - ALL WORLD IS STAGE

1.3 Playfair

Playfair - simmetric and first litteral digram substitution cipher, invented by Charles Wheatstone, but named by Lord Playfair who promoted use of that cipher. Harder to break, that single letter substitutional ciphers, cause it's harder to make frequency analysis for bigrams. Nowadays it is not used cause even smartphones easily break it in seconds.

1.3.1 Weaknesses

Plyafair is susceptitable for frequency analize, but because it is done on pairs of letters, it is significantly harder to crack. By hand this task in merely imposible, but with the help of a computer, it can be done in seconds. Another useful weakness of the Playfair Cipher is the fact that the same pair of letters reversed will produce the same pair of letters reversed in ciphertext. For example, if the plaintext "er" encrypts to "HY", then the plaintext "re" will encrypt rto "YH". This is useful in some words in english such as "departed" which start and end with the same pair of letter in reverse.

1.3.2 Encryption

To encrypt we use 5x5 square starting from keyword and finished by rest of ordered alphabet without J (suppose J==I) like:

```
S O M E K
Y A B C D
F G H I L
N P Q R T
U V W X Z
```

Also we divide our plaintext in bigrams like:

```
IN TE LX LI GE NC EX
```

If there're repeated letters or last one hasn't got pair, we add X after letter. Then we use 4 rules to crypt that message with Playfair cipher.

1. If 2 symbols of bigram stays on one row, we substitute them with right neighbors each.
2. .. stays on one col, subsitute with below letters.
3. .. stays on vertexes of rectangle, change them on letters, that stays on their row and also are vertexes of that rectangle
4. If there is no below or right side neighbor, we took first from opposite side (first row, or first col).

Let's crypt our message

1. IN stays on vertexes of F, I, X, U rectangle and we change them to FR
2. TE change to RK
3. LX = IZ
4. LI is on one row, we change them to right neighbor, i-¿L, but L is last in row, we change it to first letter: L-¿F
5. GE = IO
6. NC = RY
7. EX = CE

Decrypting goes same, but uses inversed rules.

1.4 ADFGVX

ADFGVX (ADFGX in origin) is cipher that was originally invented by Lt. Fritz Nebel and upgrageded in 1918. It uses both substitional and transpostitional methods, that made it very strong for usage in WWI. Cipher is named after six characters that used in it. Those was chosen because they look very different in Morse code, that makes errors more rare.

1.5 Comparing with Playfair

ADFGVX is more stronger then Playfair because it uses both substitutional and transpositional ways of cryptography. Also ADFGVX keyset is bgger than playfairs. Encryption Let's encrypt 'RFC'. First we need 5x5 square filled with secret mixed alphabet - substition key

```
  A D F G X
A Z X D A W
D V R T U S
F L M O Q E
G Y I P F G
X H K N B C
```

I and J encrypted like one to make 26 six alphabet fit in 25 cells.

Using that for each letter in plaintext we take row letter and column letter.
R = DD F = GG C = XX DDGGXX

Second step is transposition. We write our ciphertext under transposition key.

```
H A L F
D D G G
X X
```

Then we sort letter in HALF in alphabetical order, changing cols in table,

```
A F H L
D G D G
X   X
```

and write by columns from up to below. We got ciphertext = DX GD XG

Decryption is just inverse of each step using both keys.

1.5.1 Encrypting text with Vigenere

My plain text was

```
memories can be vile, repulsive little brutes. like children, i suppose.
haha. but can we live without them? alghough, why not? we aren't
contractually tied down to rationality! there is no sanity clause! so when
you find yourself locked onto an unpleasant train of thought, heading for
the places in your past where the screaming is unbearable, remember
there's always madness. you can just step outside, and close the door
on all those dreadful things that happened. you can lock them away.
forever. madness is the emergency exit.
```

Firstly I took out all punctuation and spaces

```
memoriescanbevilerepulsivelittlebruteslikechildrenisupposehahabut
canwelivewithoutthemalghoughwhynotwearentcontractuallytieddowntor
ationalitythereisnosanityclausesowhenyoufindyourselflockedontoanu
npleasanttrainofthoughtheadingfortheplacesinyourpastwherethescrea
mingisunbearableremembertheresalwaysmadnessyoucanjuststepoutsidea
ndclosethedooronallthosedreadfulthingsthathappenedyoucanlockthema
wayforevermadnessistheemergencyexit
```

Key=JOKER, after multiplying to length of ciphertext mod length of key, i have

```
JOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJO
KERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKE
RJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJ
OKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOK
ERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKER
JOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJOKERJO
KERJOKERJOKERJOKERJOKER
```

Using Vigener's square I took column marked as encrypting letter, and row marked with letter that stays whos position is same as encrypting letter.

```
vswsirscgrwpozzusbigdzcmmnzsxkuslvlcscpztsmlzurbiergetgxgolrqolykl
oxavuwfinrhrslchridjzqlfdurayhbyxnnobiecqyrkaomxljzvckrsnhffbdsijh
ssejzsxpcvovvrgxsjjbsxplzkyjngyaynbislowxhpxibwvutvsttsnsecckrl
wdvirboxxkaosrfohrslpvdlvjrsrxocbxyndvetngsrpxibtrbhglvasdlvbqbirv
wxkzbixfvjfkfcnfoqvvpovkqsbijjzgepbakhengccfdqkradgdwkndyykbwnirwr
mpfbsdlvmcyvfwovpkqcciuaskhwdzdlzwucxyjhregysxiuhcegrwzygbcvoqrfoi
jfasfiivonrvbgswkqsoqvauorthshmk
```

1.5.2 Decrypting Vigener

I got this ciphertext:

```
BUWCMKJILBMFMCWSNMQOJKXLBHWMUVAJKWZPICMMHPCSVLTLQZUCJXCHKZHJMVSA
SNQLNWKJLRASFXUFRBXGVGMSLLEYEBNPGPWMHXQAIIIFGOJQSQGUTZBRQPFZLIEB
EWEMOLKCJGQGDMKAQNQOFHDOJQGCAFHCEQWHZKTRQBSGSWYYCTMFMMNAEITGRVGR
MYJUJEOCJWGCWSYVWJKLJBXVIZUZWWHLFUMFMYFGLGGHKCKWWSYVWVQFVBAYBPWM
HXCHRTRQQFMOKLCXZVIMTVYWUENUELFGTVYOJCCZWIBPAVSHZMUMVKMGWABSEIPN
ZWGYNRBCLLGLYQLRWENQSPJCXPEGOUYGXVQGKPXNIFYQWRVOIGYMZZTFWSPNYMAG
AGTFQSHWIGIRWTWOHLANYMUCAGXCMVEYZADYPAXTSWECEIMGVTGCGO
```

Firstly i tried to find length of key.

1.6 Encrypting with chosen cipher

I chose Affien cipher and keys a=5 and b=7. Plaintext

```
There's a time when the operation of the machine becomes so odious, makes you so sick at heart, t
```

After processing like in vigenere, we got

```
theresatimewhentheoperationofthemachinebecomessoodiousmakesyousosickatheart
thatyoucanttakepartyoucantevenpassivelytakepartandyouvegottoputyourbodiesup
onthegearsanduponthewheelsupontheleversuponalltheapparatusandyouvegottomake
itstopandyouvegottoindicatetothepeoplewhorunittothepeoplewhoownitthatunless
yourefreethemachinewillbepreventedfromworkingatall
```

Converted to numbers

```
19 7 4 17 4 18 0 19 8 12 4 22 7 4 13 19 7 4 14 15 4 17 0 19 8 14 13 14 5
19 7 4 12 0 2 7 8 13 4 1 4 2 14 12 4 18 18 14 14 3 8 14 20 18 12 0 10 4 18
24 14 20 18 14 18 8 2 10 0 19 7 4 0 17 19 19 7 0 19 24 14 20 2 0 13 19 19
0 10 4 15 0 17 19 24 14 20 2 0 13 19 4 21 4 13 15 0 18 18 8 21 4 11 24 19
0 10 4 15 0 17 19 0 13 3 24 14 20 21 4 6 14 19 19 14 15 20 19 24 14 20 17
```

1 14 3 8 4 18 20 15 14 13 19 7 4 6 4 0 17 18 0 13 3 20 15 14 13 19 7 4 22
7 4 4 11 18 20 15 14 13 19 7 4 11 4 21 4 17 18 20 15 14 13 0 11 11 19 7 4
0 15 15 0 17 0 19 20 18 0 13 3 24 14 20 21 4 6 14 19 19 14 12 0 10 4 8 19
18 19 14 15 0 13 3 24 14 20 21 4 6 14 19 19 14 8 13 3 8 2 0 19 4 19 14 19
7 4 15 4 14 15 11 4 22 7 14 17 20 13 8 19 19 14 19 7 4 15 4 14 15 11 4 22
7 14 14 22 13 8 19 19 7 0 19 20 13 11 4 18 18 24 14 20 17 4 5 17 4 4 19 7
4 12 0 2 7 8 13 4 22 8 11 11 1 4 15 17 4 21 4 13 19 4 3 5 17 14 12 22 14
17 10 8 13 6 0 19 0 11 11

Each number we process through affine function

$$E(x) = (ax + b) mod m \tag{6}$$

24 16 1 14 1 19 7 24 21 15 1 13 16 1 20 24 16 1 25 4 1 14 7 24 21 25 20 25
6 24 16 1 15 7 17 16 21 20 1 12 1 17 25 15 1 19 19 25 25 22 21 25 3 19 15
7 5 1 19 23 25 3 19 25 19 21 17 5 7 24 16 1 7 14 24 24 16 7 24 23 25 3 17
7 20 24 24 7 5 1 4 7 14 24 23 25 3 17 7 20 24 1 8 1 20 4 7 19 19 21 8 1 10
23 24 7 5 1 4 7 14 24 7 20 22 23 25 3 8 1 11 25 24 24 25 4 3 24 23 25 3 14
12 25 22 21 1 19 3 4 25 20 24 16 1 11 1 7 14 19 7 20 22 3 4 25 20 24 16 1
13 16 1 1 10 19 3 4 25 20 24 16 1 10 1 8 1 14 19 3 4 25 20 7 10 10 24 16 1
7 4 4 7 14 7 24 3 19 7 20 22 23 25 3 8 1 11 25 24 24 25 15 7 5 1 21 24 19
24 25 4 7 20 22 23 25 3 8 1 11 25 24 24 25 21 20 22 21 17 7 24 1 24 25 24
16 1 4 1 25 4 10 1 13 16 25 14 3 20 21 24 24 25 24 16 1 4 1 25 4 10 1 13
16 25 25 13 20 21 24 24 16 7 24 3 20 10 1 19 19 23 25 3 14 1 6 14 1 1 24
16 1 15 7 17 16 21 20 1 13 21 10 10 12 1 4 14 1 8 1 20 24 1 22 6 14 25 15
13 25 14 5 21 20 11 7 24 7 10 10

And convert to characters like we done earlier

yqbobthyvpbnqbuyqbzebohyvzuzgyqbphrqvubmbrzpbttzzwvzdtphfbtxzdtztvrfhyqbhoy
yqhyxzdrhuyyhfbehoyxzdrhuybibuehttvibkxyhfbehoyhuwxzdiblzyyzedyxzdomzwvbtde
zuyqblbhothuwdezuyqbnqbbktdezuyqbkbibotdezuhkkyqbheehohydthuwxzdiblzyyzphfb
vytyzehuwxzdiblzyyzvuwvrhybyzyqbebzekbnqzoduvyyzyqbebzekbnqzznuvyyqhydukbtt
xzdobgobbyqbphrqvubnvkkmbeobibuybwgozpnzofvulhyhkk