187 - Day 03

Friday, April 6, 2018 8:40 AM

Day 03 – Classical Cryptosystems (cont.)

Last time

- Generalize mono-alphabetic subs.
  (Caesar shift w/o keeping the ABC order)
  $|K| = 26!$
- Vigenere cipher : need a keyword of length N.
  use multiple Caesar shifts.
  Ex : Keyword : YES
  Y- shift for every $1^{st}, 4^{th}, 7^{th}, 10^{th} \ldots$ letters
  E - shift ——— $2^{nd}, 5^{th}, 8^{th} \ldots$
  S - shift ——— $3^{rd}, 6^{th}, 9^{th}, \ldots$
  $|K| = 26^N$
- Rectangular Transposition :
  Put p/t into a rectangle & rearrange the columns.
- Playfair. Construct a Playfair square using a keyword.
  + put I/J in the same cell.
  + letters in keyword first, omit any repeat.
  + the rest of the alphabet.

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

Encrypt : Same row : shift right (GK → HL, CF → DB)
Same col : shift down (PU → UO, AR → EX)
Corner : replace with the other corner
(PE : C ← E, P → R ⇒ RC)

Decrypt : . same row : shift left
. same col : shift up.
. corner : same

ADFGVX cipher

- The ADFGVX system was introduced by the German Colonel Fritz Nebel.
- It was broken by Georges Painvin in one of the all-time most remarkable feats of cryptanalysis.
- It was not until December 1962 that the feat of Painvin was made known.
- It permitted the French to block the last German offensive of 1918.
- ADFGVX can be seen as a combination between Playfair cipher and rectangular transposition.

Playfair + Rec. Trans.

Encryption process:

1. Construct a 6×6 ADFGVX matrix with entries taken from 26 alphabet letters and 10 number digits
2. Convert each letter in the plaintext into its coordinates in the ADFGVX table. Coordinates are ordered as (row index, column index).
3. Rearrange the converted text (**row-by-row from left to right**) into a table with n columns and permute the columns using a chosen permutation of length n.
4. Read the permuted table column-by-column from top to bottom to obtain the ciphertext

4. Read the permuted table column-by-column from top to bottom to obtain the ciphertext

2

Construct table from a keyword

- 26 letters A,..., Z
- 10 digits 0,..., 9
- Keyword: SUMMER

	A	D	F	G	V	X
A	S	U	M	E	R	A
D	B	C	D	F	G	H
F	I	J	K	L	N	O
G	P	Q	T	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Example. Encrypt the following message "*from one day to another in battle*" using the permutation 8 4 3 2 7 6 1 5 and the table

	A	D	F	G	V	X
A	i	w	o	u	l	d
D	e	f	r	y	0	a
F	9	b	c	1	g	h
G	j	k	2	m	n	7
V	p	3	q	s	6	t
X	4	v	x	5	z	8

(row, col)

$|K| = 36!$

"x" → XF

f	r	o	m	o	n	e	d	a	y
DD	DF	AF	GG	AF	GV	DA	AX	DX	DG

t	o	a	n	o	t	h	e	r
VX	AF	DX	GV	AF	VX	FX	DA	DF

i	n	b	a	t	t	l	e
AA	GV	FD	DX	VX	VX	AV	DA

8	4	3	2	7	6	1	5
D	D	D	F	A	F	G	G
A	F	G	V	D	A	A	X
D	X	D	G	V	X	A	F
D	X	G	V	A	F	V	X
F	X	D	A	D	F	A	A
G	V	F	D	D	X	V	X
V	X	A	V	D	A	X	F

use image of 'x' as a filler

GAAVAVX FVGVADV DGDGDFA

DFXXXVX ...

3

Decryption process:

1. Fill the letters of the cipher-text into a table of n columns, where n is the length of the permutation. We fill the entries **column-by-column**, **top-to-bottom**, and **left-to-right**.
2. Label each column from left to right with $1, 2, \ldots, n$. Then rearrange the columns so that the given permutation appears.
3. Read the text from step 2 **row-by-row**, **left-to-right**, and **top-to-bottom**. Then break the resultant text into pairs.
4. Translate each pair into the plaintext using its coordinates in the ADFGVX table. Coordinates are ordered as (row index, column index).

Vernam cipher

Theorem 1 (Quotient-Remainder Theorem). *Given an integer A and a positive integer B. Then there exist integers q, r (obtained through long division) such that $A = B \cdot q + r$ where $0 \le r < B$.*

Here, q is **quotient** *and r is* **remainder**. *We say $r = A \mod B$*

Example.

- $\overbrace{521}^{A} = \overbrace{26}^{B} \times \underbrace{20}_{\text{quotient}} + \underbrace{1}_{\text{remainder}}$

- $-521 = -26 \times 20 - 1 = 26 \times (-20) + (-1)$

$$= 26 \times (-20) + 26 + (-1) - 26$$

$$= 26 \times \underbrace{(-21)}_{q} + \underbrace{25}_{r}$$

$521 = 1 \mod 26$

$-521 = 25 \mod 26.$

- $521 + 264 \pmod{26}$

$= 1 + 4 \pmod{26}$

$= 5 \pmod{26}$

$264 = 26 \times 10 + 4$

$264 = 4 \mod 26$

$139 = 26 \times 5 + 9$

$787 = 26 \times 30 + 7$

- $139 \times 787 \pmod{26}$

$= 9 \times 7 \pmod{26}$

$= 63 \pmod{26} = 11 \pmod{26}$

Original Vernam cipher uses binary string

XOR

Vernam cipher - Encryption process:

- Translate the given plaintext into numbers $A \to 0, B \to 1, \ldots, Z \to 25$.
- Randomize two short keys U and V and compute the long key V, as follows

perfect secrecy.

$$K(i) = U(i) + V(i) \mod 26$$

for each $1 \leq i \leq n$ where n is the length of the plaintext.

- Compute $C(i) := M(i) + K(i) \mod 26$, for each i, and use substitute each $M(i)$ by the corresponding letter in the alphabet.

Example. Encrypt the message **NO MORE AMMO** using the keys $\{U, V\} = \{(3, 1, 2), (7, 3, 8, 4, 5)\}$

Solution. The long key K is

U	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
V	7	3	8	4	5	7	3	8	4	5	7	3	8	4	5
K	10	4	10	7	6	9	6	9	6	8	...				

U + V mod 26

Decrypt:

$M = C - K$ mod 26

Plaintext	N	O	M	O	R	E	A	M	M	O
M	13	14	12	14	17	4	0	12	12	14
K	10	4	10	7	6	9	6	9	6	8
C	23	18	22	21	23					
Ciphertext	X	S	W	V	X					

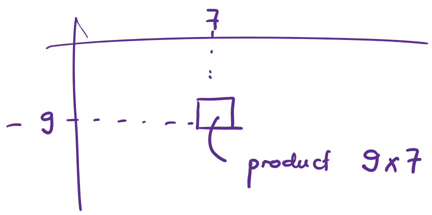
C = M + K mod 26

$$2\left(\frac{1}{2}\right) = 1$$

$\frac{1}{2} = 2^{-1}$ is the inverse of 2

Definition 1 (Inverse in modular arithmetic). *If $A \cdot C = 1 \mod B$ then C is the modular inverse of A under mod B. Denote $C = A^{-1} \mod B$*

Use the multiplication table to find the inverses under mod 26



product 9×7 mod 26.

Inverses of (under mod 26)

5 $\rightarrow$	$5^{-1} = 21$	$21^{-1} = 5$
16 $\rightarrow$	D.N.E	
23 $\rightarrow$	$23^{-1} = 17$	$17^{-1} = 23$
24 $\rightarrow$	D.N.E	

to find inverse of 5, look at row 5 and find a "1" entry in the table.

- If there's a "1" $\rightarrow$ look up the column number to get the inverse
- If there's no "1" then the inverse D.N.E.