Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-01-22

Recap

- Two methods for attacking the Vigenère cipher
  - Frequency analysis
  - Dot Product
- Playfair Cipher

Classical Cryptosystems - Section 2.6

ADFGX CIPHER

ADFGX Cipher

- Invented by Colonel Fritz Nebel in 1918
- Used by the German army on the Western front during World War I
- Successfully attacked by French cryptanalyst Georges Painvin
- ADFGX are easy to distinguish in Morse code:

  A: · —   D: — · ·   F: · · — ·   G: — — ·   X: — · · —

  reducing transmission errors, an early attempt to combine *encryption* and *error correction*.
- ADFGX was eventually replaced by the ADFGVX cipher

Polybius square (~200BC)

- A **Polybius square** (or **checkerboard**) is a device used to *fractionate* plaintext characters so that they can be represented by a smaller set of symbols.

- Each letter is coded as its corresponding *row* and *column* symbol

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Example:

`peachykeen` $\longmapsto$ `35 15 11 13 23 54 25 15 15 33`

ADFGX Cipher

- <u>Encryption</u>:
  1. Code message using a random Polybius square with labels ADFGX:

	A	D	F	G	X
A	x	g	a	d	s
D	t	i/j	q	e	p
F	h	c	u	r	z
G	y	f	k	m	w
X	n	b	v	o	l

Plaintext: `t h e k n i g h t s w h o s a y n i`

Code: `DAFADGGFXADDADFADAAXGXFAXGAXAFGAXADD`

ADFGX Cipher

Codetext: `DAFADGGFXADDADFADAAXGXFAXGAXAFGAXADD`

2. Choose a word as a Key and arrange the Codetext into blocks of whatever size the keyword is.

Key:

P	Y	T	H	O	N
D	A	F	A	D	G
G	F	X	A	D	D
A	D	F	A	D	A
A	X	G	X	F	A
X	G	A	X	A	F
G	A	X	A	D	D

ADFGX Cipher

3. Sort columns according to the alphabetic order of the key word.

P	Y	T	H	O	N
D	A	F	A	D	G
G	F	X	A	D	D
A	D	F	A	D	A
A	X	G	X	F	A
X	G	A	X	A	F
G	A	X	A	D	D

$\Longrightarrow$

H	N	O	P	T	Y
A	G	D	D	F	A
A	D	D	G	X	F
A	A	D	A	F	D
X	A	F	A	G	X
X	F	A	X	A	G
A	D	D	G	X	A

4. Cipher text is formed by read down the columns:

ciphertext: AAAXXAGDAAFDDDDFADDGAAXGFXFGAXAFDXGA

ADFGX Cipher

Decryption: Reverse the process.

	A	D	F	G	X
A	x	g	a	d	s
D	t	i/j	q	e	p
F	h	c	u	r	z
G	y	f	k	m	w
X	n	b	v	o	l

key: `yep`

ciphtertext:
`GFAXGDAAGDGDDAFXAXAX`

- Figure out column lengths: ciphertext = 20 letters key = 3 letters

$$20 = \mathbf{6} \cdot 3 + \mathbf{2}$$

There will be $\mathbf{6}$ rows of three letters and one row of $\mathbf{2}$ letters, i.e., the 'p' column will have one less letter.

ADFGX Cipher

Ciphertext:

GFAXGDAAGDGDDAFXAXAX

key:

yep

- Place letters into columns:

E	P	Y
G	A	A
F	G	F
A	D	X
X	G	A
G	D	X
D	D	A
A		X

⟹

Y	E	P
A	G	A
F	F	G
X	A	D
A	X	G
X	G	D
A	D	D
X	A	

Polybuis square:

	A	D	F	G	X
A	x	g	a	d	s
D	t	i/j	q	e	p
F	h	c	u	r	z
G	y	f	k	m	w
X	n	b	v	o	l

Codetext:

AGAFFGXADAXGXGDADDXA

Plaintext:

d a r n t o o t i n

Classical Cryptosystems - Section 2.7

BLOCK CIPHERS

Block Cipher

- Plaintext is grouped into “blocks” which are encrypted as a whole
  - Typically, changing one letter changes the whole block

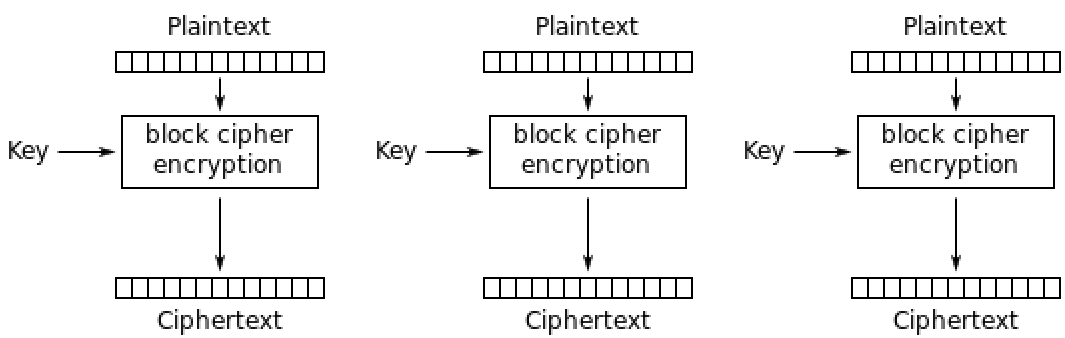
- Makes frequency analysis more difficult

Examples:

- Playfair (blocks of size 2)
- DES (64 bit blocks)
- AES (128 bit blocks)

Block Cipher Mode of Operation

- **Electronic Codebook Mode (ECB):**
  - Blocks are encoded individually one at a time



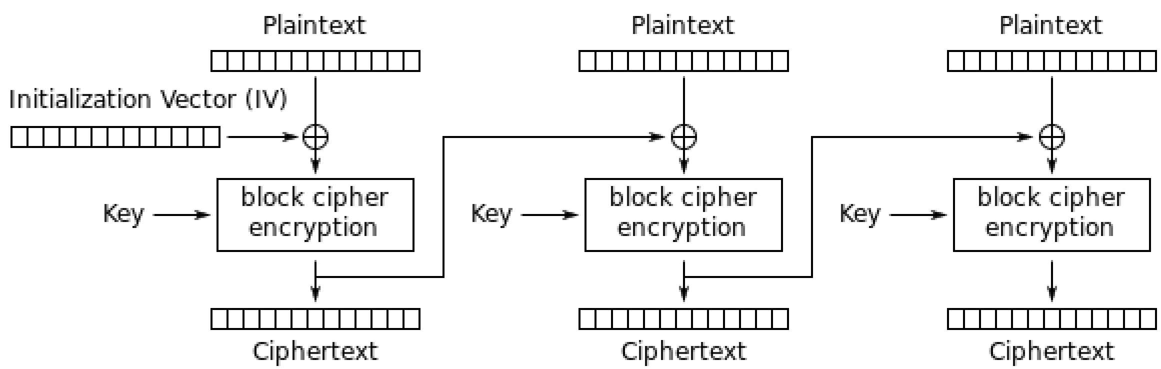
Electronic Codebook (ECB) mode encryption

- Not recommended by *anyone*!

(Wikipedia, Block cipher mode of operation)

Block Cipher Mode of Operation

- **Cipher Block Chaining (CBC):**
  - Use information from the previously ciphered block to code the next block before encrypting

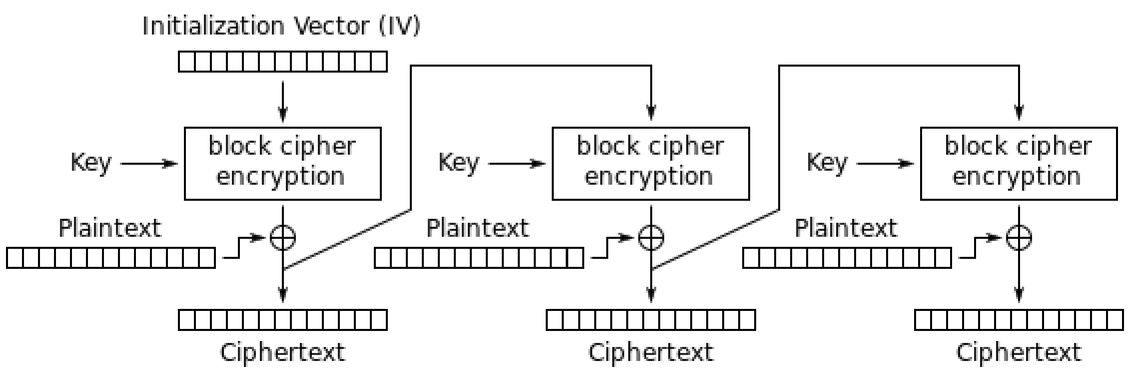


Cipher Block Chaining (CBC) mode encryption

(Wikipedia, Block cipher mode of operation)

Block Cipher Mode of Operation

- **Cipher Feedback (CBF):**
  - Information from the previously ciphered block and the plaintext are used to code the next block before encrypting



Cipher Feedback (CFB) mode encryption

(Wikipedia, Block cipher mode of operation)

Block Cipher Mode of Operation

- **Other Modes:**
  - Propagating cipher-block chaining (PCBC)
  - Output feedback (OFB)
  - Counter (CTR)

(Wikipedia, Block cipher mode of operation)

Hill Cipher (1929)

- Invented by Lester Hill
- Never in widespread use
- Probably the first time algebra was used in an essential way
- Algebra is essential to most modern cryptographic systems

Hill Cipher

1. Pick $n \in \mathbb{Z}$. Create an $n \times n$ matrix with entries modulo 26.

Example: $n = 3$

$$\begin{pmatrix} 3 & 22 & 17 \\ 8 & 2 & 11 \\ 23 & 5 & 19 \end{pmatrix}$$

2. Split message into blocks of size n and encode as an integer-valued vectors:

Example:

`seespotrunxx` $\longmapsto$ `(18,4,4),(18,15,14),(19,17,20),(13,23,23)`

Hill Cipher

- Encryption:
  - Multiple coded vector by matrix (mod 26)

Coded Vectors: $(18,4,4),\ (18,15,14),\ (19,17,20),\ (13,23,23)$

$$(18 \quad 4 \quad 4)\begin{pmatrix} 3 & 22 & 17 \\ 8 & 2 & 11 \\ 23 & 5 & 19 \end{pmatrix} = (178 \quad 424 \quad 426) \equiv (22 \quad 8 \quad 10) \pmod{26}$$

$$(18 \quad 15 \quad 14)\begin{pmatrix} 3 & 22 & 17 \\ 8 & 2 & 11 \\ 23 & 5 & 19 \end{pmatrix} = (496 \quad 496 \quad 737) \equiv (2 \quad 2 \quad 9) \pmod{26}$$

$$(19 \quad 17 \quad 20)\begin{pmatrix} 3 & 22 & 17 \\ 8 & 2 & 11 \\ 23 & 5 & 19 \end{pmatrix} = (653 \quad 552 \quad 890) \equiv (3 \quad 6 \quad 6) \pmod{26}$$

$$(13 \quad 23 \quad 23)\begin{pmatrix} 3 & 22 & 17 \\ 8 & 2 & 11 \\ 23 & 5 & 19 \end{pmatrix} = (752 \quad 447 \quad 911) \equiv (24 \quad 5 \quad 1) \pmod{26}$$

Encrypted Vectors: $(22,8,10),\ (2,2,9),\ (3,6,6),\ (24,5,1)$

Ciphertext: W I K C C J D G G Y F B

Inverse of a Matrix $(\mathbf{mod}\ n)$

- The inverse of the matrix M, notated M^{-1}, is the matrix such that

$$M\,M^{-1} \equiv I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \pmod{n}$$

- For vectors v and w, if

$$v\,M \equiv w \pmod{n}$$

then

$$v \equiv v\,I \equiv v\,(M\,M^{-1}) \equiv (v\,M)\,M^{-1} \equiv w\,M^{-1} \pmod{n}$$

Basic Number Theory - Section 3.8

INVERTING MATRICES MOD N

Inverse of a 2x2 Matrix

For $a, b, c, d \in \mathbb{R}$ such that $ad - bc \neq \mathbf{0}$, if

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then

$$M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

<u>Check</u>:

$$(ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Inverse of a 2x2 Matrix $(\bmod n)$

Similarly,

$$(ad-bc)^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n}$$

if $(ad-bc)^{-1} \pmod{n}$ exists, i.e., when

$$\gcd(ad-bc, n) = 1.$$

In fact, $M^{-1} (\bmod n)$ exists if $\det M \not\equiv 0 \pmod{n}$.

Determinant of $k \times k$ Matrix

Expansion of Co-factors:

$$\det\begin{pmatrix} \boldsymbol{a} & b & c & \cdots & d \\ \boldsymbol{e} & f & g & \cdots & h \\ \boldsymbol{i} & j & k & \cdots & l \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{m} & n & o & \cdots & p \end{pmatrix}$$

$$= a\det\begin{pmatrix} f & g & \cdots & h \\ j & k & \cdots & l \\ \vdots & \vdots & \ddots & \vdots \\ n & o & \cdots & p \end{pmatrix} - e\det\begin{pmatrix} b & c & \cdots & d \\ j & k & \cdots & l \\ \vdots & \vdots & \ddots & \vdots \\ n & o & \cdots & p \end{pmatrix} + i\det\begin{pmatrix} b & c & \cdots & d \\ f & g & \cdots & h \\ \vdots & \vdots & \ddots & \vdots \\ n & o & \cdots & p \end{pmatrix}$$

$$- \cdots$$

Determinant of $k \times k$ Matrix

Expansion of Co-factors:

$$\det\begin{pmatrix} 2 & 8 & 11 \\ 1 & 3 & 7 \\ 5 & 5 & 4 \end{pmatrix}$$

$$= 2\det\begin{pmatrix} 3 & 7 \\ 5 & 4 \end{pmatrix} - \det\begin{pmatrix} 8 & 11 \\ 5 & 4 \end{pmatrix} + 5\det\begin{pmatrix} 8 & 11 \\ 3 & 7 \end{pmatrix}$$

$$= 2\,(-23) - (-23) + 5\,(23) = 92$$

Inverse of a $k \times k$ Matrix $(\mathrm{mod}\ n)$

<u>Gauss-Jordan elimination method</u>:

Turn

$$\left(\begin{array}{cccc|cccc} a & b & \cdots & c & 1 & 0 & \cdots & 0 \\ d & e & \cdots & f & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h & i & \cdots & j & 0 & 0 & \cdots & 1 \end{array}\right) \quad \text{into} \quad \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & A & B & \cdots & C \\ 0 & 1 & \cdots & 0 & D & E & \cdots & F \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & H & I & \cdots & J \end{array}\right)$$

using the rules:

1. Multiply a row by a constant $\qquad r_1 \to c\, r_1$
2. Swap two rows $\qquad r_1 \to r_2,\ r_2 \to r_1$
3. Replace a row with the sum of another row $\qquad r_1 \to r_1 + r_2$

Rules 1. and 3. can be combined to give $\qquad r_1 \to c\, r_1 + d\, r_2$

Inverse of a $k \times k$ Matrix $(\mathrm{mod}\ n)$

Example:

$$\left(\begin{array}{cc|cc} 7 & 3 & 1 & 0 \\ 5 & 6 & 0 & 1 \end{array}\right) \xrightarrow{r_1 \to 7^{-1} r_1} \left(\begin{array}{cc|cc} 1 & 19 & 15 & 0 \\ 5 & 6 & 0 & 1 \end{array}\right) \pmod{26} \qquad 7^{-1} \equiv 15 \pmod{26}$$

$$\xrightarrow{r_2 \to 5^{-1} r_2} \left(\begin{array}{cc|cc} 1 & 19 & 15 & 0 \\ 1 & 22 & 0 & 21 \end{array}\right) \pmod{26} \qquad 5^{-1} \equiv 21 \pmod{26}$$

$$\xrightarrow{r_2 \to r_2 - r_1} \left(\begin{array}{cc|cc} 1 & 19 & 15 & 0 \\ 0 & 3 & 11 & 21 \end{array}\right) \pmod{26}$$

$$\xrightarrow{r_2 \to 3^{-1} r_2} \left(\begin{array}{cc|cc} 1 & 19 & 15 & 0 \\ 0 & 1 & 21 & 7 \end{array}\right) \pmod{26} \qquad 3^{-1} \equiv 9 \pmod{26}$$

$$\xrightarrow{r_1 \to r_1 - 19\, r_2} \left(\begin{array}{cc|cc} 1 & 0 & 6 & 23 \\ 0 & 1 & 21 & 7 \end{array}\right) \pmod{26}$$

<u>Check</u>: $\begin{pmatrix} 7 & 3 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 6 & 23 \\ 21 & 7 \end{pmatrix} = \begin{pmatrix} 105 & 182 \\ 156 & 157 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$ ✓

Hill Cipher Example

Similarly, with a little work:

$$\left(\begin{array}{ccc|ccc} 3 & 22 & 17 & 1 & 0 & 0 \\ 8 & 2 & 11 & 0 & 1 & 0 \\ 23 & 5 & 19 & 0 & 0 & 1 \end{array}\right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 11 & 9 & 0 \\ 0 & 1 & 0 & 5 & 2 & 19 \\ 0 & 0 & 1 & 10 & 5 & 6 \end{array}\right) \pmod{26}$$

which means that if

$$\begin{pmatrix} a & b & c \end{pmatrix} \begin{pmatrix} 3 & 22 & 17 \\ 8 & 2 & 11 \\ 23 & 5 & 19 \end{pmatrix} \equiv \begin{pmatrix} A & B & C \end{pmatrix} \pmod{26}$$

then

$$\begin{pmatrix} a & b & c \end{pmatrix} \equiv \begin{pmatrix} A & B & C \end{pmatrix} \begin{pmatrix} 11 & 9 & 0 \\ 5 & 2 & 19 \\ 10 & 5 & 6 \end{pmatrix} \pmod{26}$$

Over the Hill Cipher

- <u>Decryption</u>:
  - Multiply the encrypted vectors by the inverse matrix:

Encrypted Vectors: $(22,8,10),\ (2,2,9),\ (3,6,6),\ (24,5,1)$

$$\begin{pmatrix}22 & 8 & 10\end{pmatrix}\begin{pmatrix}11 & 9 & 0\\ 5 & 2 & 19\\ 10 & 5 & 6\end{pmatrix} \equiv \begin{pmatrix}18 & 4 & 4\end{pmatrix} \pmod{26}$$

$$\begin{pmatrix}2 & 2 & 9\end{pmatrix}\begin{pmatrix}11 & 9 & 0\\ 5 & 2 & 19\\ 10 & 5 & 6\end{pmatrix} \equiv \begin{pmatrix}18 & 15 & 14\end{pmatrix} \pmod{26}$$

$$\begin{pmatrix}3 & 6 & 6\end{pmatrix}\begin{pmatrix}11 & 9 & 0\\ 5 & 2 & 19\\ 10 & 5 & 6\end{pmatrix} \equiv \begin{pmatrix}19 & 17 & 20\end{pmatrix} \pmod{26}$$

$$\begin{pmatrix}24 & 5 & 1\end{pmatrix}\begin{pmatrix}11 & 9 & 0\\ 5 & 2 & 19\\ 10 & 5 & 6\end{pmatrix} \equiv \begin{pmatrix}13 & 23 & 23\end{pmatrix} \pmod{26}$$

Decrypted Vectors: $(18,4,4),\ (18,15,14),\ (19,17,20),\ (13,23,23)$

Plaintext: S E E S P O T R U N X X