Classical Encryption Techniques

Jibi Abraham

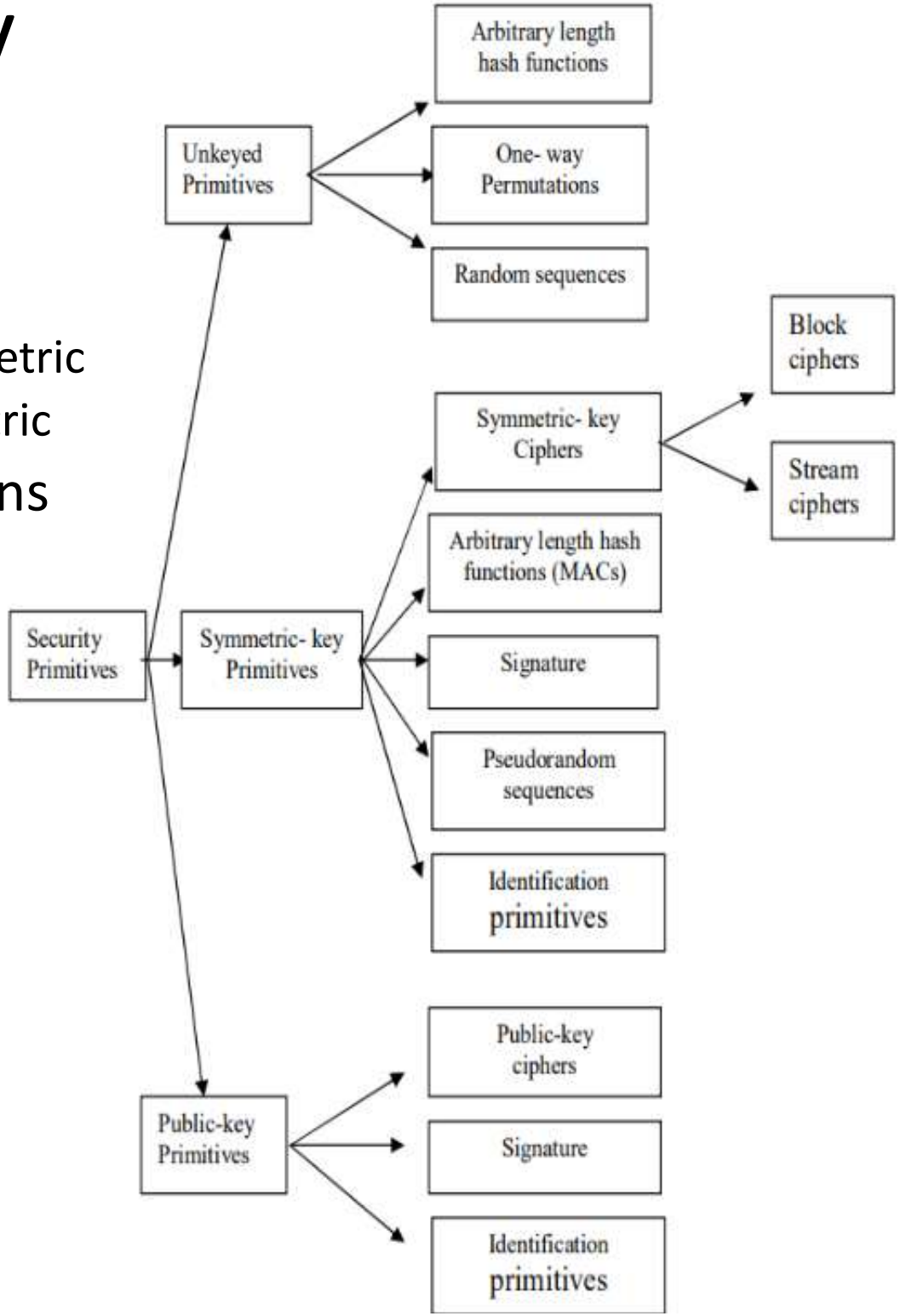
COEP TECHNOLOGICAL UNIVERSITY

Shivajinagar, Pune-411 005

(A Unitary Technological University of Govt. of Maharashtra)

Cryptography

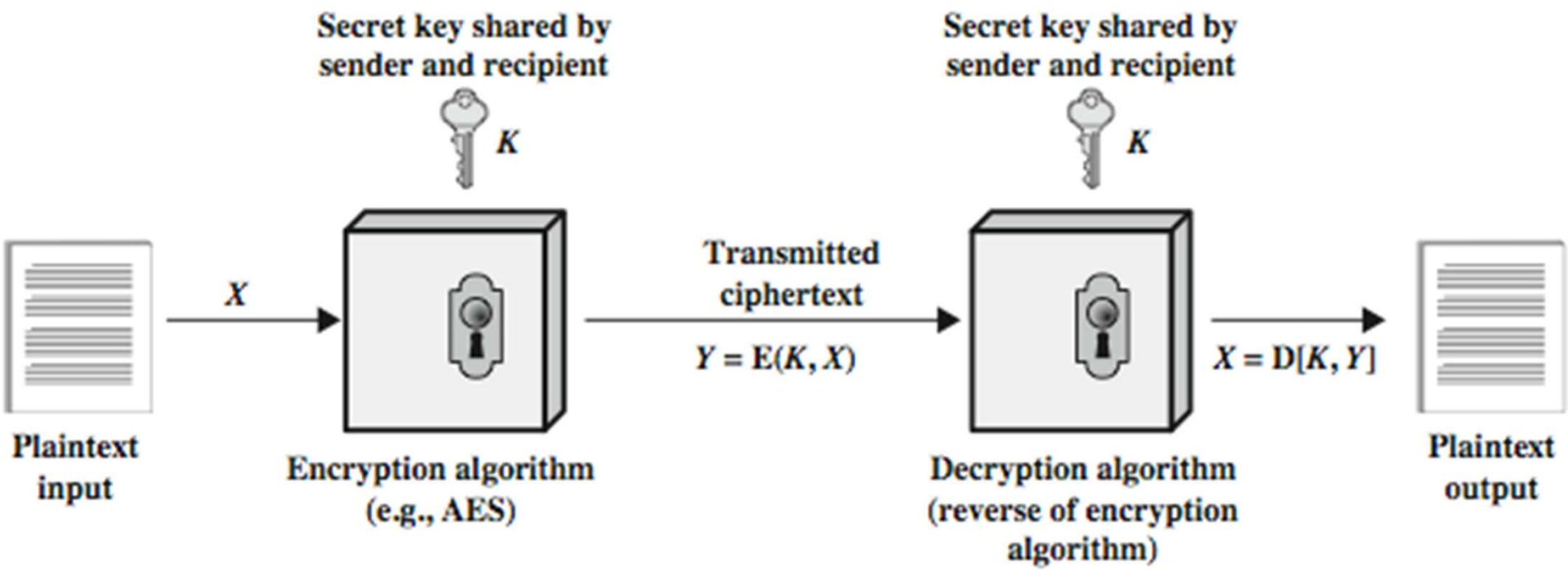
- Characterize cryptographic system by:
  - Number of keys used
    - single-key or private or symmetric
    - two-key or public or asymmetric
  - Type of encryption operations used
    - Substitution
    - Transposition
    - Product of substitution and transposition
  - Way in which plaintext is processed
    - Block
    - Stream



Symmetric Encryption

- Also known as conventional / private-key / single-key encryption
- Sender and recipient share a common key
- All classical encryption algorithms are private-key
- Was only type prior to invention of public-key in 1970's
- And by far most widely used (still)
- Is significantly faster than public-key crypto

Symmetric Cipher Model



- Some Basic Terminology
  - **plaintext** - original message
  - **ciphertext** - coded message
  - **cipher** - algorithm for transforming plaintext to ciphertext
  - **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Cipher - Requirements

- Two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- Mathematically have:
  - $Y = E(K, X) = E_K(X) = \{X\}_K$
  - $X = D(K, Y) = D_K(Y)$
- Assume encryption algorithm is known
  - Kerckhoff's Principle: security in secrecy of key alone, not in obscurity of the encryption algorithm
- Implies a secure channel to distribute key
  - Central problem in symmetric cryptography

Cryptanalysis

- Objective to recover key not just message
- General approaches:
  - Brute-force attack
  - Cryptanalytic attack
    - Plaintext/Cipher Text available based Analysis
  - Modern attacks
    - Man-in-the-Middle attack
    - Side-channel attack
    - Differential cryptanalysis
- If either succeeds, all key use compromised

Cryptanalytic Attacks

1. **Ciphertext only**
   - Only know the algorithm and many ciphertexts
   - Feasible with brute force, but impractical if the key size is large
   - Knowing the type of plaintext (e.g. English), by statistical analysis (dictionary attack) can identify plaintext
2. **Known plaintext**
   - Know/suspect a few plaintext and corresponding ciphertext
   - Eg. A file encoded in pdf always begins with the same format
3. **Chosen plaintext**
   - Attacker selects plaintext and obtains its ciphertext
   - E.g. in 1990, using differential cryptanalysis, DES was broken with an effort of $O(2^{47})$
4. **Chosen ciphertext**
   - Select ciphertext and obtain plaintext
   - Primarily applicable to Public key systems, happened with RSA
5. **Chosen text**
   - Select plaintext or ciphertext to en/decrypt
   - Very uncommon

Cipher Strength

- **Unconditional security**
  - No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
    - Only one-time pad
- **Computational security**
  - Meeting the criteria
    - Cost of breaking the cipher exceeds the value of the encrypted information
    - Time required to break the cipher exceeds the useful lifetime of the encrypted information

Complexity of an Attack

- Is measured as
  - Data Complexity: the amount of data needed as input to the attack
  - Processing Complexity: Time and computing power needed to perform the attack
  - Storage Complexity: Memory required to perform the attack

Classical Substitution Ciphers

- Where letters of plaintext are replaced by other letters or by numbers or symbols
- Or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
- Hill Cipher
- Vigenère Cipher
- Autokey Cipher
- Vernam Cipher
- Vigenère Cipher
- Autokey Cipher
- Vernam Cipher

Familiar Number Systems

- Groups, Rings and Fields are concerned with sets on whose elements we can operate algebraically
- Perform an operation of two elements of the set and to obtain a third element of the same set itself
-

$$\mathbb{N} = \{0, 1, 2, \dots\} \quad \text{the natural numbers}$$
$$\mathbb{Z} = \{\, m - n \mid m, n \in \mathbb{N} \,\} \quad \text{the integers}$$
$$\mathbb{Q} = \{\, m/n \mid m, n \in \mathbb{Z},\ n \neq 0 \,\} \quad \text{the rational numbers}$$
$$\mathbb{R} \quad \text{the real numbers}$$
$$\mathbb{C} \quad \text{the complex numbers}$$

Number Theory: Modulo Operation

- **Definition:** Let $a, r, m \in Z$ (where Z is a set of all integers) and $m > 0$
- $r \equiv$ a mod m if m divides $r - a$.
- m is called the *modulus*, r is called the *remainder*
- $a = q \cdot m + r \qquad 0 \leq r < m$
- **Example:** $a = 42$ and $m = 9$
  - $42 = 9 \cdot 4 + 6$ therefore $42 \equiv 6 \bmod 9$
- What is 134 mod 5?
  - Ans: 4

Negative number modulo

- -x mod n?
- First find the largest number y, that is less than or equal to -x and divisible by n
- Rem = x-y
- Example: -7 mod 5
  - 5x(-2)+3 = -7
  - -7 mod 5 = 3
- What is -255 mod 11?
  - $-255 = (-24 \times 11) + 9$

Caesar Cipher

- Earliest known substitution cipher designed by Julius Caesar used in military affairs
- Also known as shift cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$c = E(k, p) = (p + k) \bmod (26)$

$p = D(k, c) = (c - k) \bmod (26)$

- What is 'howdy' encrypted using key *f* (a shift of 5)?
  - (7,14,22,3,24) + 5 = MTBID

Caesar Cipher

$c = E(k, p) = (p + k) \bmod (26)$

$p = D(k, c) = (c - k) \bmod (26)$

- Example k = 3:
  - meet me after the toga party
  - PHHW PH DIWHU WKH WRJD SDUWB
- What key do we need to make CAESAR become MKOCKB?
  - using a key 10

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Cryptanalysis of Caesar Cipher

- Only have 26 possible ciphers
  - A maps to A,B,..Z
- Could simply try each in turn by a **brute force search**
- Given ciphertext, just try all shifts of letters
- Do need to recognize when have plaintext
- **Example:**
- Ciphertext : R K K R T B (17, 10, 10, 17, 19, 1)
- Perform Brute force.
- When the key k = 17
- Plaintext = A T T A C K = (0, 19, 19, 0, 2, 10)

Affine Cipher

- Broaden to include multiplication
- key $k=(\alpha, \beta)$
- Can define affine transformation as:
  - $c = E(k, p) = (\alpha p + \beta) \bmod (26)$
  - $p = D(k, c) = \alpha^{-1} (c - \beta) \bmod (26)$

Affine Cipher – Encryption Example

- k=(α, β), c = E(k, p) = ($\alpha p + \beta$) mod (26)

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25

- example: encryption of the plaintext “sail” with encryption key (3,7)

$$
\begin{aligned}
\text{s} &\longrightarrow 18 \longrightarrow 3 \cdot 18 + 7 \equiv 9 \pmod{26} \longrightarrow \text{J} \\
\text{a} &\longrightarrow 0 \longrightarrow 3 \cdot 0 + 7 \equiv 7 \pmod{26} \longrightarrow \text{H} \\
\text{i} &\longrightarrow 8 \longrightarrow 3 \cdot 8 + 7 \equiv 5 \pmod{26} \longrightarrow \text{F} \\
\text{l} &\longrightarrow 11 \longrightarrow 3 \cdot 11 + 7 \equiv 14 \pmod{26} \longrightarrow \text{O}
\end{aligned}
$$

Affine Cipher – Decryption

- $c = E(k, p) = (\alpha p + \beta) \bmod (26)$
- $p = D(k, c) = \alpha^{-1} (c - \beta) \bmod (26)$
- α must be relatively prime to 26 so there exists unique inverse α^{-1}
- Relatively Prime numbers: two or more integers that have only 1 as a greatest common divisor (GCD)
- The numbers need not have to be prime
- Eg: 45 = 1 x 32x 5

  91 = 1 x 7 x 13

  GCD(45, 91) = 1

Inverse modulo

- Given two integers **A** and **M**, what is A^{-1} mod M?
- Let X = A^{-1} mod M, then $AX \equiv 1 \bmod M$
- Multiplicative inverse of "A modulo M" exists if and only if A and M are relatively prime (i.e. if gcd(A, M) = 1)
- Example:
  - 3^{-1} mod 11
    - = 4 (3*4 mod 11 = 1)
  - 10^{-1} mod 17
    - = 12 (10*12 mod 17 = 1)

Affine Cipher – Decryption Example

- key k=(α, β)

$c = E(k, p) = (\alpha p + \beta) \bmod (26)$

$p = D(k, c) = \alpha^{-1} (c - \beta) \bmod (26)$

- Ciphertext: QTORHG was produced using an affine cipher with encryption key (3,7). What is plaintext?
- $3^{-1} \bmod 26 = 9$
- $-7 \bmod 26 = (26x(-1)+19) = 19$

Q → 16 → 9(16+19) mod 26 = 3 → D

T → 19 → 9(19+19) mod 26 = 4 → E

O → 14 → 9(14+19) mod 26 = 11 → L

R → 17 → 9(17+19) mod 26 = 12 → M

H → 7 → 9(7+19) mod 26 = 0 → A

- Decrypt "ENBHW" with key (3, 1)?
  - (9, -1) = (9, 25) ="BEACH"

Security of Affine Cipher

- **Example:** $k = (\alpha, \beta) = (13, 4)$
  - INPUT = (8, 13, 15, 20, 19) $\Rightarrow$ ERRER
  - ALTER = (0, 11, 19, 4, 17) $\Rightarrow$ ERRER
- There is no one-to-one map between plaintext and ciphertext space. What went wrong?
- **Key Space:** β can be any number in Z_{26}. So, 26 possibilities
- Since α^{-1} has to exist we can only select integers in Z_{26} such that gcd(α, 26) = 1.
- α candidates are {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}
- Therefore, the key space has $12 \cdot 26 = 312$ candidates

Monoalphabetic Cipher

- Each plaintext letter maps to a different random ciphertext letter arbitrarily

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

- Plaintext and Ciphertext

P	i	f	w	e	w	i	s	h	t	o	r	e	p	l	a	c	e	l	e	t	t	e	r	s
C	w	i	r	f	r	w	a	j	u	h	y	f	t	s	d	v	f	s	f	u	u	f	y	a

Monoalphabetic Cipher Security

- Key space is 26! = 4 x 10^{26} keys
- With so many keys, might think it is secure
- The problem is language characteristics
- English Letter Frequencies

a:	8.05%	b:	1.67%	c:	2.23%	d:	5.10%
e:	12.22%	f:	2.14%	g:	2.30%	h:	6.62%
i:	6.28%	j:	0.19%	k:	0.95%	l:	4.08%
m:	2.33%	n:	6.95%	o:	7.63%	p:	1.66%
q:	0.06%	r:	5.29%	s:	6.02%	t:	9.67%
u:	2.92%	v:	0.82%	w:	2.60%	x:	0.11%
y:	2.04%	z:	0.06%				

8.1: Letter frequencies in the book *The Adventures of Tom Sawyer*, by Twain.

Statistics for Digrams and Trigrams

- Equally powerful statistical inferences can be made by comparing the relative frequencies for pairs and triples of characters in the ciphertext and the language believed to be used for the Plaintext
- Pairs of adjacent characters are referred to as digrams, and triples of characters as trigrams.
- The most frequently occurring trigrams ordered by decreasing frequency are:

  the and ent ion tio for nde .....
- If we have the relative frequencies for all possible digrams available, we can represent this table by the joint probability p(x, y) where x denotes the first letter of a digram and y the second letter.
- Such joint probabilities can be used to compare the digram-based statistics of ciphertext and plaintext.

Digram Frequencies

digram	*frequency*	*digram*	*frequency*	*digram*	*frequency*	*digram*	*frequency*
th	3.15	to	1.11	sa	0.75	ma	0.56
he	2.51	nt	1.10	hi	0.72	ta	0.56
an	1.72	ed	1.07	le	0.72	ce	0.55
in	1.69	is	1.06	so	0.71	ic	0.55
er	1.54	ar	1.01	as	0.67	ll	0.55
re	1.48	ou	0.96	no	0.65	na	0.54
es	1.45	te	0.94	ne	0.64	ro	0.54
on	1.45	of	0.94	ec	0.64	ot	0.53
ea	1.31	it	0.88	io	0.63	tt	0.53
ti	1.28	ha	0.84	rt	0.63	ve	0.53
at	1.24	se	0.84	co	0.59	ns	0.51
st	1.21	et	0.80	be	0.58	ur	0.49
en	1.20	al	0.77	di	0.57	me	0.48
nd	1.18	ri	0.77	li	0.57	wh	0.48
or	1.13	ng	0.75	ra	0.57	ly	0.47

Use in Cryptanalysis

- Monoalphabetic substitution ciphers do not change relative letter frequencies
- Calculate letter frequencies for ciphertext and compare counts against known values
- Tables of common 2/3 letters (digrams/trigrams) help
- Given ciphertext:
  - UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  - VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  - EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- Guess P and Z are e and t
- Guess ZW is th and hence ZWP is “the”
- Proceeding with trial and error finally get:
  - it was disclosed yesterday that several informal but
  - direct contacts have been made with political
  - representatives of the viet cong in moscow

Playfair Cipher

- The large number of keys in a monoalphabetic cipher not even provide security
- **Playfair Cipher** is invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair
- Consider ways to reduce the "spikyness" of natural language text, since if just map one letter always to another, the frequency distribution is just shuffled
- Playfair cipher encrypts more than one letter at once
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

Playfair Cipher

- Encrypts a letter to multiple letters
- a 5X5 matrix of letters is formed based on a key
  - Remove duplicate letters in the key
  - Fill key letters in the Matrix L to R, top to bottom
  - I/J used as a single letter
  - Fill rest of matrix with other letters
- eg. using the keyword MONARCHY

M	O	N	A	R
C	H	Y		

Encrypting and Decrypting

- Plaintext is encrypted two letters at a time
  1. If a pair is a repeated letter, insert filler like ‘X’
  2. If both letters fall in the same row, replace each with a letter to right (wrapping back to start from end)
  3. If both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
  4. Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Playfair Example

- Message = Move forward
- Plaintext = mo ve fo rw ar dx
- Here x is just a filler, the message is padded and segmented
- mo -> ON; ve -> UF; fo -> PH, etc.
- Ciphertext = ON UF PH NZ RM BZ

M	O	N	A	R
C	H	Y		

Playfair Decryption Example

- Decrypt VR FK AF GO NV NB UL LM IZ IH IE FE SH ZX using the key “ANOTHER”
- WE LI VE IN AW OR LD FU LX LO FB EA UT YX

Security of Playfair Cipher

- Security much improved over monoalphabetic since have 26 x 26 = 676 digrams
- Would need a 676 entry frequency table to analyse (versus 26 for a monoalphabetic) and correspondingly more ciphertext
- was widely used for many years
  - eg. by US and British military in World War -1
- It **can** be broken,
  - Same pair is converted always to same pair ciphertext
  - count the frequencies of pairs of letters
  - The higher frequency pairs may correspond to commonly occurring pair of letters in English text like THE, AT, TO

Greatest Common Divisor (gcd)

- Definition: Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called the greatest common divisor of a and b. The greatest common divisor is denoted as gcd(a,b).
- gcd(24,36) = 12
- Let $a=p_1^{a1}p_2^{a2}p3^{a3}\ldots p_k^{ak}$ and $b= p_1^{b1}p_2^{b2}p3^{b3}\ldots p_k^{bk}$
- $gcd(a, b)= p_1^{min(a1,b1)}p_2^{min(a2,b2)}p_3^{min(a3,b3)}\ldots p_k^{min(ak,bk)}$
- gcd(24,36) = ?
- $24 = 2*2*2*3=2^3*3^1$
- $36= 2*2*3*3=2^2*3^2$
- $gcd(24,36) =2^2*3^1 = 12$

Euclid's Algorithm

- Uses theorem that:
- GCD(a, b) = GCD(b, a mod b)
- Euclid's Algorithm to compute GCD(a, b) is:

```
Euclid(a, b)
    if (b= =0) then return a;
    else return Euclid(b, a mod b);
```

GCD Example

- Example GCD(1970,1066)

GCD(a, b) = GCD(b, a mod b)

```
1970 = 1 x 1066 + 904      gcd(1066, 904)
1066 = 1 x 904 + 162       gcd(904, 162)
904 = 5 x 162 + 94         gcd(162, 94)
162 = 1 x 94 + 68          gcd(94, 68)
94 = 1 x 68 + 26           gcd(68, 26)
68 = 2 x 26 + 16           gcd(26, 16)
26 = 1 x 16 + 10           gcd(16, 10)
16 = 1 x 10 + 6            gcd(10, 6)
10 = 1 x 6 + 4             gcd(6, 4)
6 = 1 x 4 + 2              gcd(4, 2)
4 = 2 x 2 + 0              gcd(2, 0)
```

GCD(1970,1066) = 2

Extended Euclidean Algorithm

- For any non-negative integers, a and b, there exist integers x and y such that: ax+ by =GCD(a, b)
- gcd(120, 84)=120x+84y
  - 120=84(1)+36
  - 84=36(2)+12
  - 36=12(3)+0
  - gcd(120, 84)= 12
- We could observe that
  - 12=84+36(-2)
  - =84+(120+84(-1))(- 2)
  - =84(3)+120(-2)

```
def xgcd(a,b):
    prevx, x = 1, 0;  prevy, y = 0, 1
    while b:
        q = a/b
        x, prevx = prevx - q*x, x
        y, prevy = prevy - q*y, y
        a, b = b, a % b
    return a, prevx, prevy
```

- follow the sequence of divisions for GCD but at each step i, keep track of x and y:
- r= ax +by
- at the end find GCD value and also x and y
- if GCD(a, b)= 1, then then x is inverse of a mod b

Extended Euclidean Algorithm

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = GCD(m, b); no inverse
3. if B3 = 1
   return B3 = GCD(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Example

Find 550^{-1} mod 1759

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = GCD(m, b); no inverse
3. if B3 = 1
   return B3 = GCD(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

Hill Cipher

- Substitute m successive plaintext letter with m ciphertext letters
- E.g. Takes three-letter combinations to the same size combinations, e.g. “the” → “rqv”
- A “block” cipher encrypting a block of text at a time
- Encryption algorithm:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26$$

where $K = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}$ is the key and det k≠0 mod 26

- Decryption algorithm:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \bmod 26$$

- Key space = 26^{m^2}

Hill Cipher - Example

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \pmod{26}$$

$$C1 = 9*p1 + 18*p2 + 10*p3 \pmod{26}$$

$$C2 = 16*p1 + 21*p2 + 1*p3 \pmod{26}$$

$$C3 = 5*p1 + 12*p2 + 23*p3 \pmod{26}$$

Hill Cipher - Example

- P = I can't do it (8 2 0 13 19 3 14 8 19)

$$\begin{pmatrix} 4 \\ 14 \\ 12 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 8 \\ 2 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 19 \\ 12 \\ 14 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 13 \\ 19 \\ 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 18 \\ 21 \\ 9 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 14 \\ 8 \\ 19 \end{pmatrix} \pmod{26}$$

C → EOM TMY SVJ

Hill Cipher - Bad Key Matrix

- Generalize key matrix to any size, matrix must be invertible

bcd → XJR

hfa → XJR

$$\begin{pmatrix} 23 \\ 9 \\ 17 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 22 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 23 \\ 9 \\ 17 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 22 \end{pmatrix} \begin{pmatrix} 7 \\ 5 \\ 0 \end{pmatrix} \pmod{26}$$

Determinant of a Matrix

- The determinant of the 2 X2 matrix

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

- Example,

$$A = \begin{bmatrix} 12 & -2 \\ 3 & 4 \end{bmatrix}$$

$$|A| = = 12(4) - (-2)(3)$$
$$= 48 + 6$$
$$= 54$$

Determinant of $n \times n$ Matrix

- For any element a_{ij}, the minor M_{ij} of that element is the determinant of the resulting matrix obtained by deleting the i^{th} row and j^{th} column.

$$\begin{bmatrix} -2 & 4 & 3 \\ 1 & 8 & 2 \\ -3 & -1 & 0 \end{bmatrix}$$

$$M_{11} = \begin{vmatrix} 8 & 2 \\ -1 & 0 \end{vmatrix} = 8(0) - (-1)(2) = 2$$

$$\begin{bmatrix} -2 & 4 & 3 \\ 1 & 8 & 2 \\ -3 & -1 & 0 \end{bmatrix}$$

$$M_{12} = \begin{vmatrix} 1 & 2 \\ -3 & 0 \end{vmatrix} = 0 + 6 = 6$$

Determinant of $n \times n$ Matrix

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 \begin{vmatrix} b_2 & c_2 \\ b_3 & c_3 \end{vmatrix} - a_2 \begin{vmatrix} b_1 & c_1 \\ b_3 & c_3 \end{vmatrix} + a_3 \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix}$$

$$= a_1 \cdot (\text{minor of } a_1) - a_2 \cdot (\text{minor of } a_2) + a_3 \cdot (\text{minor of } a_3)$$

$$\begin{bmatrix} -3 & 2 & 1 \\ 4 & 1 & -2 \\ 0 & 3 & 4 \end{bmatrix}$$

$$= -3 \begin{vmatrix} 1 & -2 \\ 3 & 4 \end{vmatrix} - 4 \begin{vmatrix} 2 & 1 \\ 3 & 4 \end{vmatrix} + 0 \begin{vmatrix} 2 & 1 \\ 1 & -2 \end{vmatrix}$$

$$= -3(4+6) - 4(8-3) = -30 - 20$$

$$= -50$$

Inverse of a Matrix

- Let A be an $n \times n$ matrix. Then A is invertible if and only if $|A| \neq 0$

$$\begin{bmatrix} -5 & 2 \\ -20 & 8 \end{bmatrix}$$

$= -40 - (-40) = -40 + 40$

$= 0$ not invertible

$$\begin{bmatrix} 12 & 0 \\ 6 & 3 \end{bmatrix}$$

$= 36 - 0 = 36$

invertible

Matrix Inverse

- Inverse of a matrix can only be defined for square matrices
- exists only if the determinant of that matrix is non-zero
- $AA^{-1} = I$

$$A^{-1} = \text{adj}(A)/\det(A)$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

2 X 2 Matrix - Example

$$K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

$$|K| = 12 - 9 = 3$$

$$\text{adj } (K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \bmod 26 = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Inverse of 3x3 Matrix

$$\text{Key} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$$

$$\det = \begin{vmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{vmatrix} = 2 \begin{vmatrix} 4 & 17 \\ 13 & 6 \end{vmatrix} - 8 \begin{vmatrix} 7 & 17 \\ 8 & 6 \end{vmatrix} + 15 \begin{vmatrix} 7 & 4 \\ 8 & 13 \end{vmatrix}$$

$$= 2\,(24 - 221) - 8\,(28 - 136) + 15(91 - 32) = 1243$$

$$1243 \times 5 \bmod 26 = 1$$

$$\det^{-1} = 5$$

COEP TECHNOLOGICAL UNIVERSITY
Shivajinagar, Pune-411 005
(A Unitary Technological University of Govt. of Maharashtra)

Inverse of 3x3 Matrix

- Find the adjoint of a matrix by taking the transpose of cofactors of the given matrix.

$$K^{-1} = \frac{1}{|D|}\,\text{adj}\,(K) = D^{-1}\,\text{adj}\,(K) = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}^{-1}$$

$$= \frac{1}{|D|}\begin{bmatrix} +(ei-fh) & -(di-fg) & +(dh-eg) \\ -(bi-ch) & +(ai-cg) & -(ah-bg) \\ +(bf-ce) & -(af-cd) & +(ae-bd) \end{bmatrix}^{T}$$

$$\therefore \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}^{-1} = 5\begin{bmatrix} +(24-221) & -(42-136) & +(91-32) \\ -(48-195) & +(12-120) & -(26-64) \\ +(136-60) & -(34-105) & +(8-56) \end{bmatrix}^{T}$$

$$= 5\begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix} \bmod 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

Hill Cipher Decryption

$$C = KP \bmod 26$$

$$P = K^{-1}C \bmod 26$$

$$k^{-1} = \frac{1}{|d|}\, adj\,[k]$$

- Example

$$\text{Key} = k = \begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

- Det(K) = 7x11 – 8x11 = -11 mod 26 = 15
- $|K|^{-1} = 7$ (15 x 7 mod 26 = 1)

Hill Cipher Decryption - Example

- K = $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

$$adj \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

- Adj(K) = $= \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} = \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} mod\ 26$

$$d^{-1} = 7$$

- K^{-1} $= 7 \times \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} = \begin{bmatrix} 77 & 126 \\ 165 & 49 \end{bmatrix} mod\ 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$

Example

- Cipher Text = $\begin{bmatrix} A \\ P \end{bmatrix}$
- $K^{-1} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$

$$P = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{bmatrix} A \\ P \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{bmatrix} 0 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{bmatrix} = \begin{bmatrix} 330 \\ 345 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix} mod\ 26 = \begin{bmatrix} S \\ H \end{bmatrix}$$

Security of Hill Cipher

- Example

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- It is easy to be broken by known plaintext attack by solve the following equation: $C_{m*m} = K_{m*m} * P_{m*m}$
- Case1: if P^{-1} exists, then $K_{m*m} = C_{m*m} * P^{-1}{}_{m*m}$
- Case2: if P^{-1} not exist, then change P and C until P^{-1} found

Polyalphabetic Ciphers

- Is a substitution cipher
- Encrypts more than one letter at once to reduce the scope of the frequency analysis of natural language text when using the Playfair cipher
- Improve security using multiple cipher alphabets
- Make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- Use a key to select which alphabet is used for each letter of the message

Vigenère Cipher

- Simplest polyalphabetic substitution cipher
- Key is multiple letters long $K = k_1\ k_2\ \ldots\ k_d$
- Repeat from start after d letters in plaintext
- eg using key = *deceptive*

K	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
K	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
P	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
P	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
C	25	8	2	21	19	22	16	39	6	17	25	6	21	19	22	26	21	25	7	28	16	24	32	37	12	32	9
C	z	i	c	v	t	w	q	n	g	r	z	g	v	t	w	a	v	z	h	c	q	y	g	l	m	g	j

- Decryption simply works in reverse

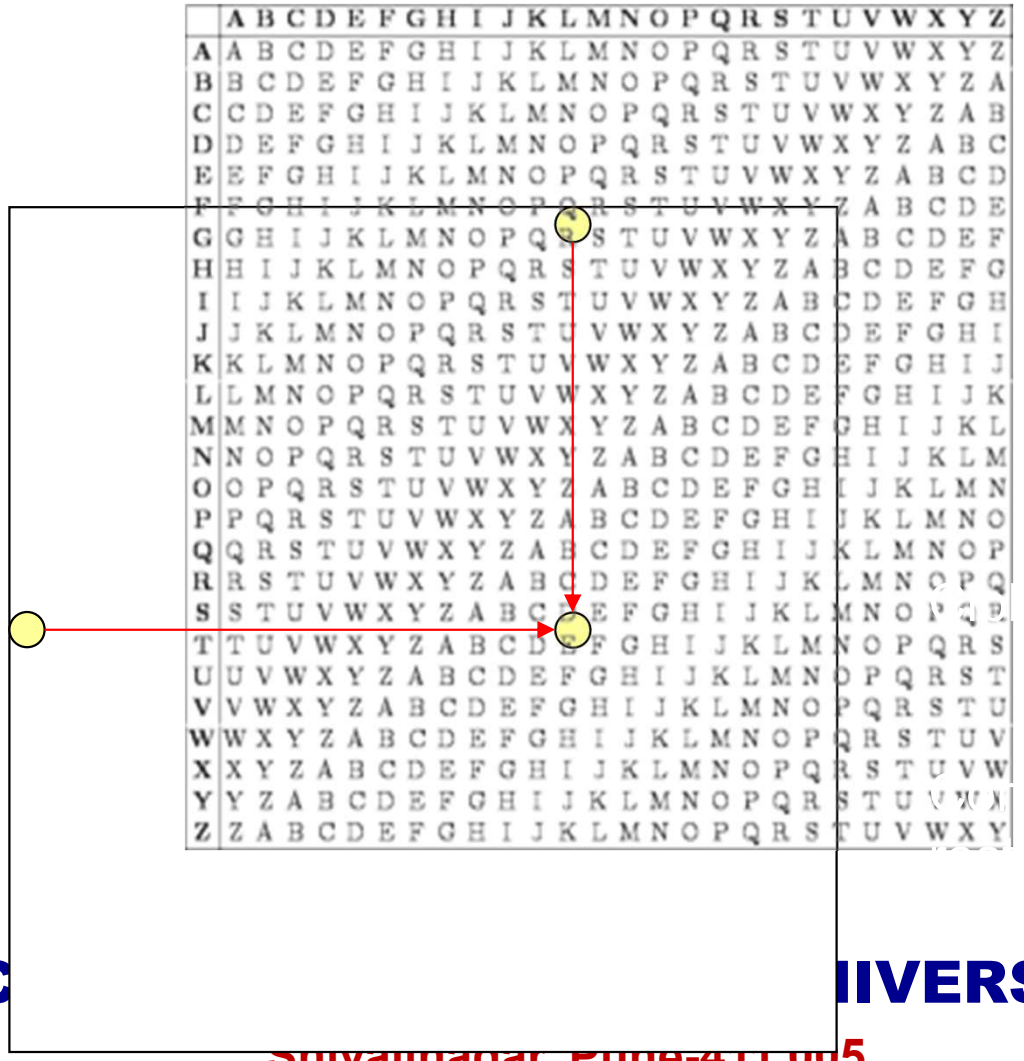
Vigenère Cipher

- need a *tabula recta.*
- To encrypt a plain text letter, you locate the row with the letter to be encrypted and the column with the corresponding letter of the key. The letter where the line and column cross is the ciphertext letter

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

Example

- Key: RESTAURANT**MEET**
- Plaintext: MEETMEFORLUNCH



Security of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter, hence letter frequencies are obscured
- But not totally lost
- Start with letter frequencies
  - see if it looks monoalphabetic or not
- If not, then need to determine number of alphabets, since then can attack each

Kasiski Attack

- Method developed by Babbage / Kasiski
- Repetitions in ciphertext give clues to period
- Find the same plaintext a multiple of key length apart which results in the same ciphertext
- Find repeated ciphertext trigrams (e.g., VTW)
- May be result of same key sequence and same plaintext sequence (or not)
- Common factors are likely key lengths

K	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
K	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
P	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
P	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
C	25	8	2	21	19	22	16	39	6	17	25	6	21	19	22	26	21	25	7	28	16	24	32	37	12	32	9
C	z	i	c	v	t	w	q	n	g	r	z	g	v	t	w	a	v	z	h	c	q	y	g	l	m	g	j

- Distance of 9 suggests key size of 3 or 9
- Then attack each monoalphabetic cipher individually using the same techniques as before

Autokey Cipher

- Autokey Cipher is almost identical to the Vigenère Cipher, but is more secure
- Ideally want a key as long as the message
- With key is prefixed to plaintext to generate key with the same size as plaintext
- eg. given key *deceptive*
  - `plaintext: wearediscoveredsaveyourself`
  - `key: deceptivewearediscoveredsav`
  - `ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA`

- Knowing key can recover the first few letters
- Use these in turn on the rest of the message
- But still have frequency characteristics to attack

Vernam Cipher

- Also known as the one-time-pad (OTP)
- The ultimate defense is to use a key as long as the plaintext
- With no statistical relationship to it
- Invented by AT&T engineer Gilbert Vernam in 1918
- Originally proposed using a very long but eventually repeating key

One-Time Pad

- If a truly random key as long as the message is used, the cipher will be secure
- Is unbreakable since ciphertext bears no statistical relationship to the plaintext
- Since for **any plaintext** and **any ciphertext** there exists a key mapping one to other
- Can only use the key **once** though
- Problems in the generation and safe distribution of key

Transposition Ciphers

- Classical **transposition** or **permutation** ciphers hide the message by rearranging the letter order without altering the actual letters used
- Can recognise these since have the same frequency distribution as the original text
- Rail Fence cipher
- Row Transposition Ciphers
- Block Transposition Ciphers

Rail Fence cipher

- Write message letters out diagonally over a number of rows
- Use a “W” pattern (not column-major)
- Then read off cipher row by row
- eg. write message out as:
  - `m e m a t r h t g p r y`
  - `e t e f e t e o a a t`
- Giving ciphertext
  - MEMATRHTGPRYETEFETEOAAT

Columnar Transposition Ciphers

- Is a more complex transposition
- Write letters of message out in rows over a specified number of columns
- Then reorder the columns according to some key before reading off the rows
  - Key: 4312567
  - Column Out 4 3 1 2 5 6 7
  - Plaintext: a t t a c k p
  - o s t p o n e
  - d u n t i l t
  - w o a m x y z
  - Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

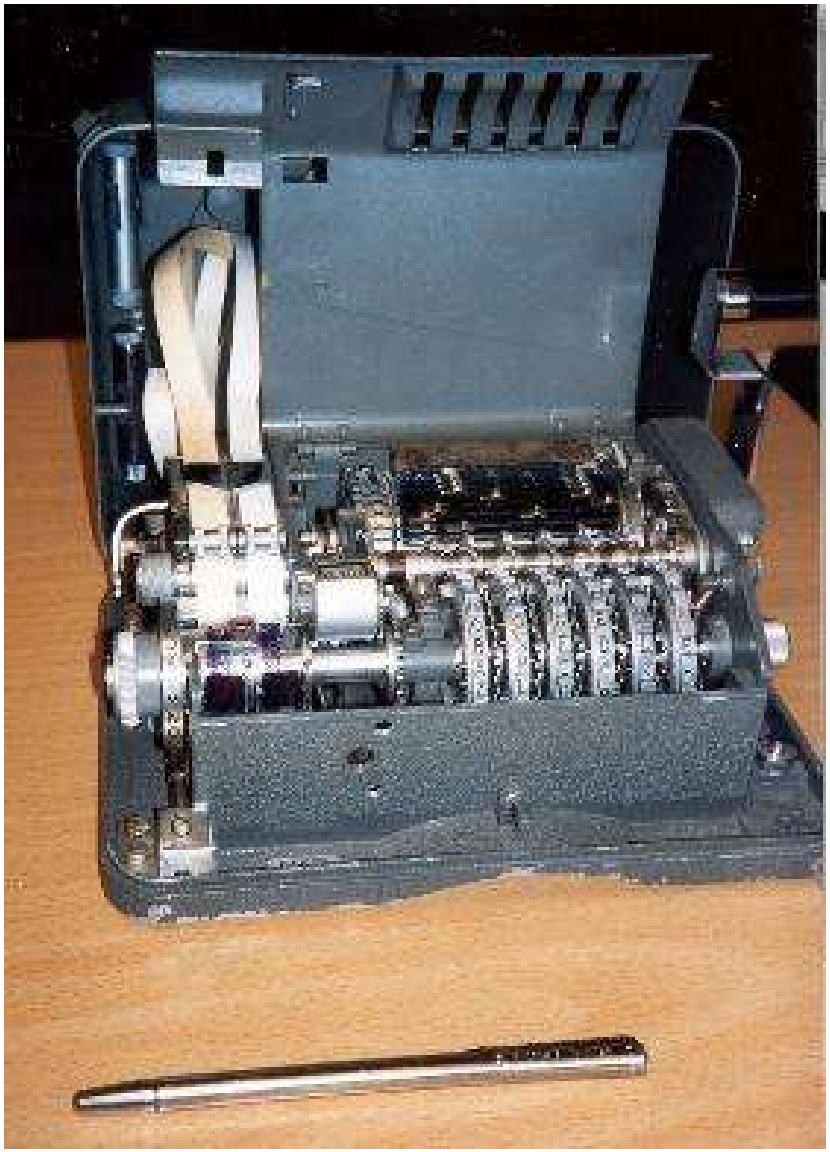
Block Transposition Ciphers

- Arbitrary block transposition may be used
- Specify permutation on block
- Repeat for each block of plaintext
  - Key: 4931285607
  - Plaintext: attackpost poneduntil twoamxyzab
  - Ciphertext: CTATTSKPAO DLEONIDUPT MBAWOAXYTZ

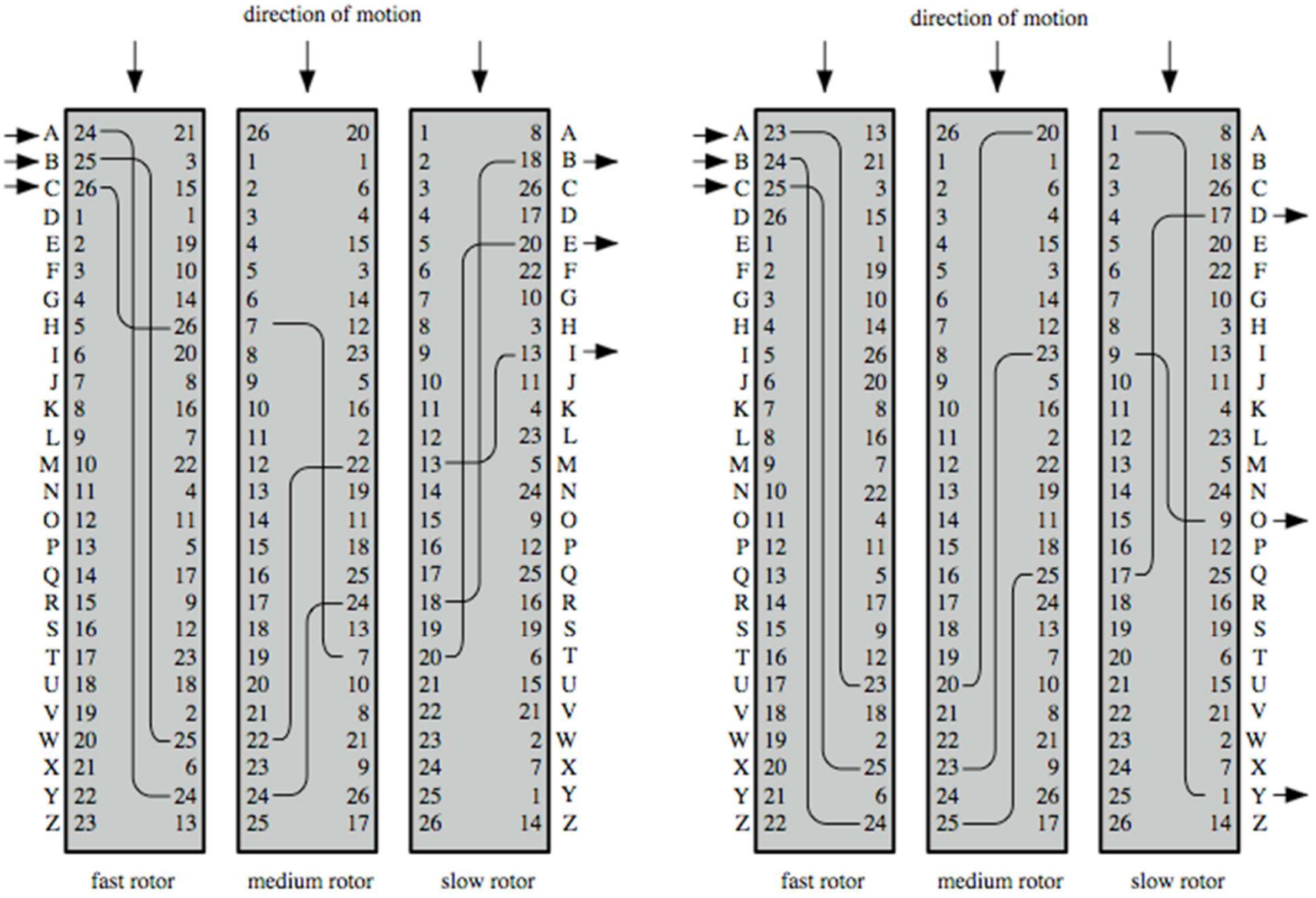
Rotor Machines

- Before modern ciphers, rotor machines were most common complex ciphers in use
- Widely used in WW2
  - German Enigma, Allied Hagelin, Japanese Purple
- Implemented a very complex, varying substitution cipher
- used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted
- with 3 cylinders have 26^3=17576 alphabets

Hagelin Rotor Machine



Rotor Machine Principles



Rotor Ciphers

- Each rotor implements some permutation between its input and output contacts
- Rotors turn like an odometer on each key stroke (rotating input and output contacts)
- Key is the sequence of rotors and their initial positions
- Note: enigma also had steckerboard permutation

Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
  - hide in “noise”
- has drawbacks
  - high overhead to hide relatively few info bits
- advantage is can obscure encryption use

Product Ciphers

- Ciphers using substitutions or transpositions are not secure because of language characteristics
- Hence consider using several ciphers in succession to make it harder, but:
  - Two substitutions make a more complex substitution
  - Two transpositions make more complex transposition
  - But a substitution followed by a transposition makes a new much harder cipher
- This is a bridge from classical to modern ciphers

Summary

- have considered:
  - classical cipher techniques and terminology
  - monoalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - Playfair cipher
  - polyalphabetic ciphers
  - transposition ciphers
  - product ciphers and rotor machines
  - steganography