جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (03)
Classical Encryption Techniques (II)

Dr. Ahmed M. ElShafee

Monoalphabetic Cipher (simple substitution cipher)

- With only 25 possible keys, the Caesar cipher is far from secure.
- A dramatic increase in the key space can be achieved by allowing an arbitrary substitution, where the translation alphabet can be any permutation of the 26 alphabetic characters (substitution box).

- Example
- Encrypt the following message

“do not go to the meeting you are discovered”

Using the following sbox

“gcbtedsmpxqwfaruohvnzkijyl”

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

ciphertext

d	o	n	o	t	g	o	t	o	t	h	e	m	e	e	t	i	n	g	y	o	u	a	r	e	d	i	s	c	o	v	e	r	e	d

Key

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
g	c	b	t	e	d	s	m	p	x	q	w	f	a	r	u	o	h	v	n	z	k	i	j	y	L

plaintext

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

ciphertext

d	o	n	o	t	g	o	t	o	t	h	e	m	e	e	t	i	n	g	y	o	u	a	r	e	d	i	s	c	o	v	e	r	e	d

Key

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
g	c	b	t	e	d	s	m	p	x	q	w	f	a	r	u	o	h	v	n	z	k	i	j	y	L

plaintext

t	r	a	r	n	s	r	n	r	n	m	e	f	e	e	n	p	a	s	y	r	z	g	h	e	t	p	v	b	r	k	e	h	e	t

- Example
- Decrypt the following message

"nmgaqvpipwwarnsr"

- Using the same sbox

"gcbtedsmpxqwfaruohvnzkijyl"

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

ciphertext

n	m	g	a	q	v	p	i	p	w	w	a	r	n	s	r

Key

g	c	b	t	e	d	s	m	p	x	q	w	f	a	r	u	o	h	v	n	z	k	i	j	y	L
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

plaintext

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

n	m	g	a	q	v	p	i	p	w	w	a	r	n	s	r

Key

g	c	b	t	e	d	s	m	p	x	q	w	f	a	r	u	o	h	v	n	z	k	i	j	y	L
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

plaintext

t	h	a	n	k	s	i	w	i	l	l	n	o	t	g	o

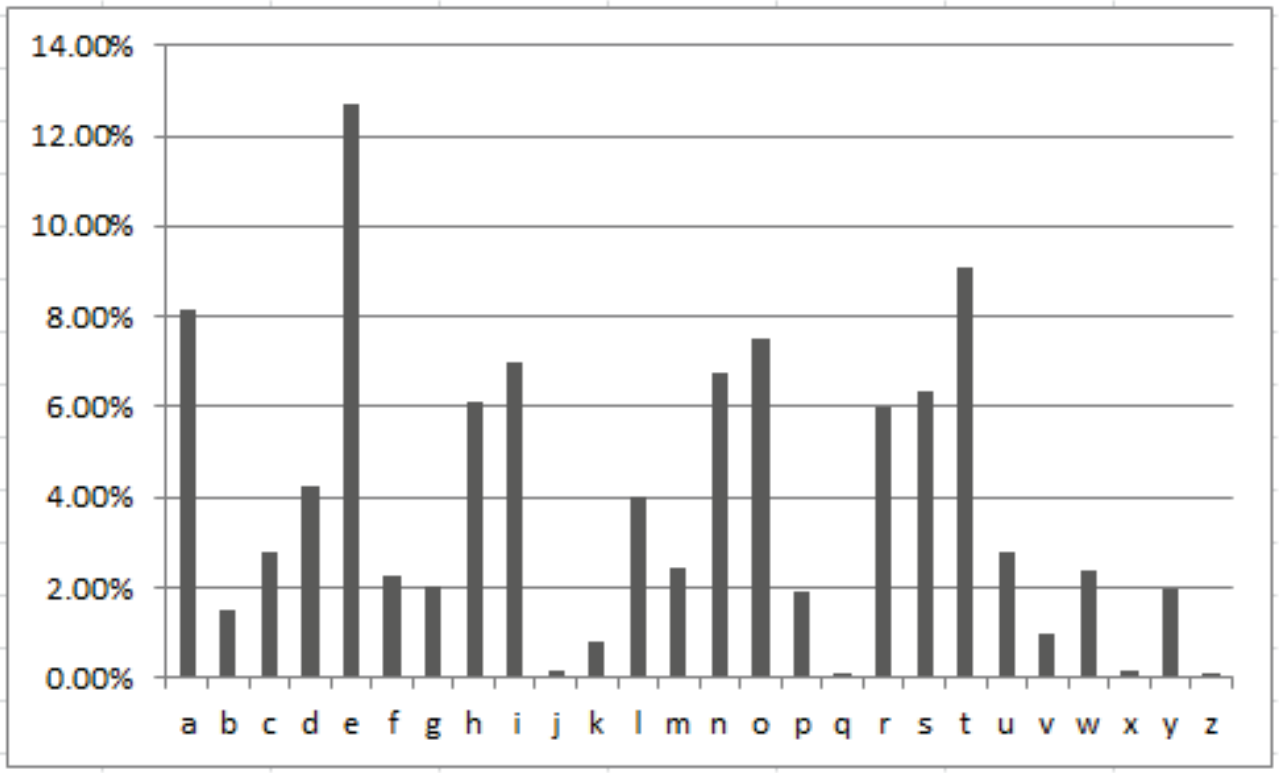
Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 10^{26} = 4 E 26 keys
- with so many keys, might think is secure

Language Redundancy and Cryptanalysis

- human languages are **redundant**
- letters are not equally commonly used
- This redundancy is also the reason we can compress text files, the computer can derive a more compact encoding without losing any information.
- in English E is by far the most common letter
  - followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages

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
8.17%	1.49%	2.78%	4.25%	12.70%	2.23%	2.02%	6.09%	6.97%	0.15%	0.77%	4.03%	2.41%	6.75%	7.51%	1.93%	0.10%	5.99%	6.33%	9.06%	2.76%	0.98%	2.36%	0.15%	1.97%	0.07%



English Letter Frequencies

Rank	Word	Rank	Word	Rank	Word	Rank	Word	Rank	Word
1	the	21	this	41	so	61	people	81	back
2	be	22	but	42	up	62	into	82	after
3	to	23	his	43	out	63	year	83	use
4	of	24	by	44	if	64	your	84	two
5	and	25	from	45	about	65	good	85	how
6	a	26	they	46	who	66	some	86	our
7	in	27	we	47	get	67	could	87	work
8	that	28	say	48	which	68	them	88	first
9	have	29	her	49	go	69	see	89	well
10	I	30	she	50	me	70	other	90	way
11	it	31	or	51	when	71	than	91	even
12	for	32	an	52	make	72	then	92	new
13	not	33	will	53	can	73	now	93	want
14	on	34	my	54	like	74	look	94	because
15	with	35	one	55	time	75	only	95	any
16	he	36	all	56	no	76	come	96	these
17	as	37	would	57	just	77	its	97	give
18	you	38	there	58	him	78	over	98	day
19	do	39	their	59	know	79	think	99	most
20	at	40	what	60	take	80	also	100	us

- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Abu al-Kindi's "A Manuscript on Deciphering Cryptographic Messages", published in the 9th century
- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- The cryptanalyst looks for a mapping between the observed pattern in the ciphertext, and the known source language letter frequencies.

- Example Cryptanalysis
- given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

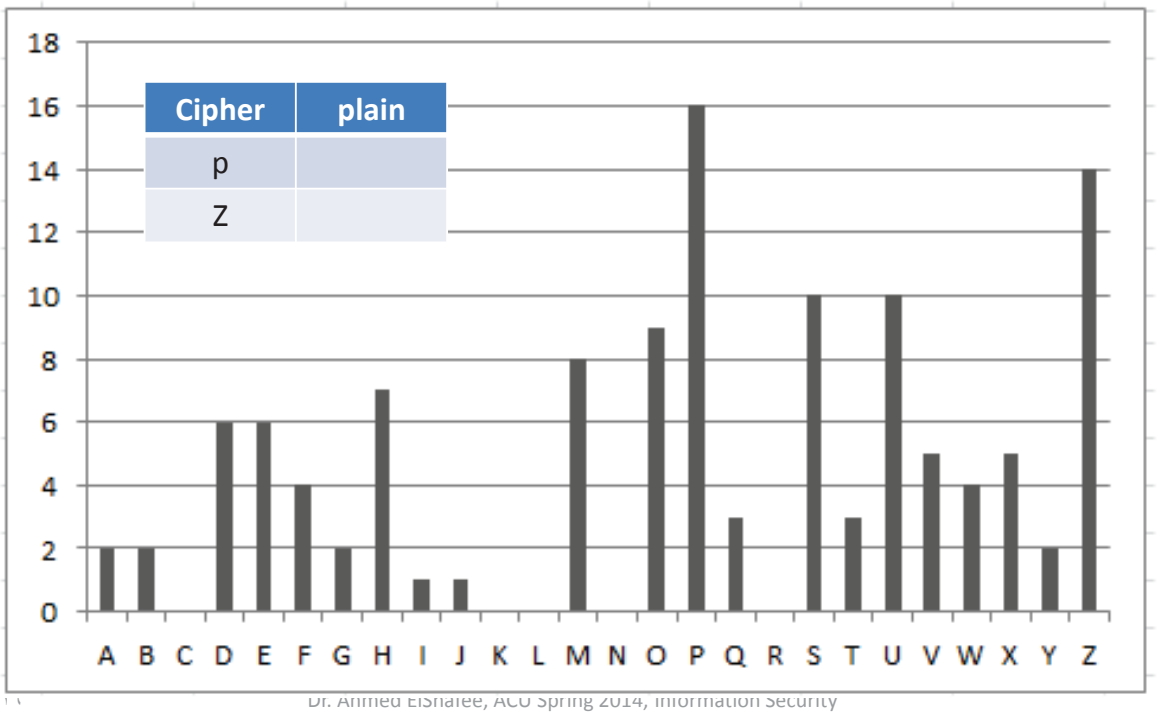
- count relative letter frequencies (see text)

Using the following online tool

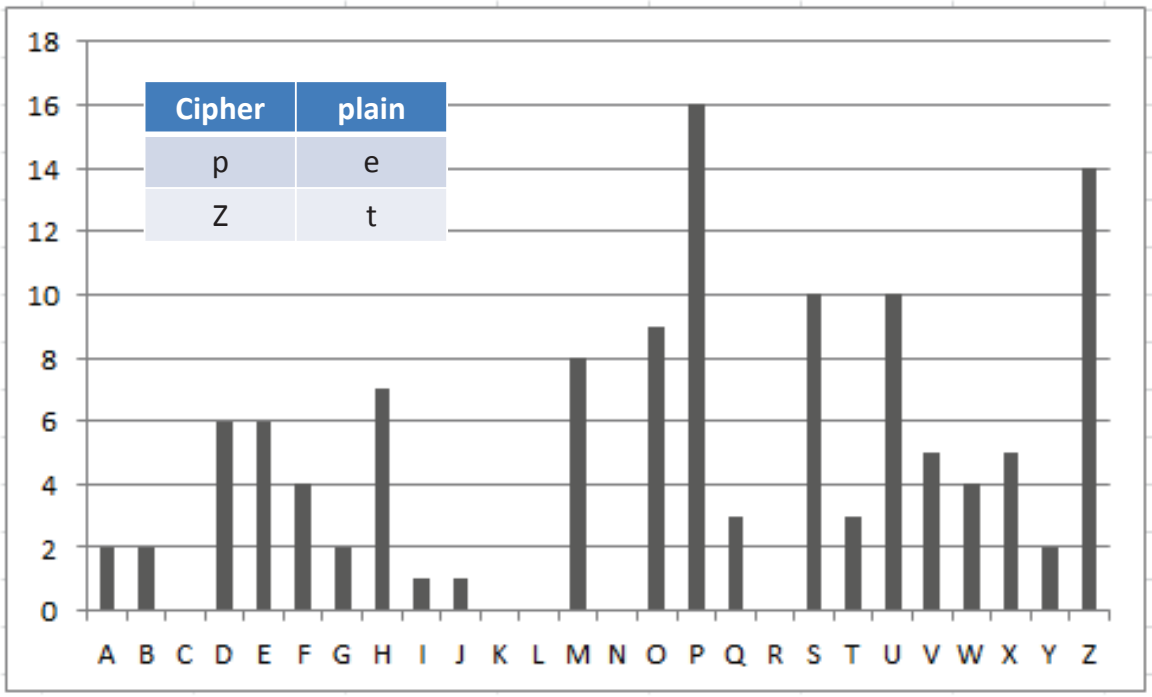
http://www.cryptool-online.org/index.php?option=com_cto&view=tool&Itemid=118&lang=en

http://www.cryptool-online.org/index.php?option=com_cto&view=tool&Itemid=113&lang=en

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
2	2	0	6	6	4	2	7	1	1	0	0	8	0	9	16	3	0	10	3	10	5	4	5	2	14



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
2	2	0	6	6	4	2	7	1	1	0	0	8	0	9	16	3	0	10	3	10	5	4	5	2	14



Cipher	plain
p	e
Z	t

Rank	Word
1	the
2	be
3	to
4	of
5	and
6	a
7	in
8	that
9	have
10	I
11	it
12	for
13	not
14	on
15	with
16	he
17	as
18	you
19	do
20	at

Cipher	plain
p	e
Z	t

FP	3	2.50%
SX	3	2.50%
PO	3	2.50%
OP	3	2.50%
UZ	3	2.50%
EP	3	2.50%
HM	3	2.50%
ZW	3	2.50%

cipher	plain
th	
it	

Cipher	plain
p	e
Z	t

FP	3	2.50%
SX	3	2.50%
PO	3	2.50%
OP	3	2.50%
UZ	3	2.50%
EP	3	2.50%
HM	3	2.50%
ZW	3	2.50%

cipher	plain
th	ZW
it	UZ

Rank	Word
1	the
2	be
3	to
4	of
5	and
6	a
7	in
8	that
9	have
10	I
11	it
12	for
13	not
14	on
15	with
16	he
17	as
18	you
19	do
20	at

Cipher	plain
p	e
Z	t

cipher	plain
th	ZW
it	UZ

cipher	plain
the	
but	

1	HMD	2	1.67%
2	DZS	2	1.67%
3	ZHM	2	1.67%
4	PZH	1	0.83%
5	UEP	1	0.83%
6	UDT	1	0.83%
7	UDB	1	0.83%
8	TSX	1	0.83%
9	UFP	1	0.83%
10	UHS	1	0.83%
11	UZU	1	0.83%
12	UZW	1	0.83%
13	UZQ	1	0.83%
14	UPZ	1	0.83%
15	UOH	1	0.83%
16	TSV	1	0.83%
17	TMO	1	0.83%
18	SOV	1	0.83%
19	QSO	1	0.83%
20	SHZ	1	0.83%
21	SGZ	1	0.83%
22	SFP	1	0.83%
23	SVP	1	0.83%
24	SXA	1	0.83%
25	VGP	1	0.83%
26	SZU	1	0.83%
27	SZO	1	0.83%
28	SXU	1	0.83%
29	SXE	1	0.83%
30	QUZ	1	0.83%
31	VUE	1	0.83%
32	ZQS	1	0.83%
33	ZSH	1	0.83%
34	ZPE	1	0.83%
35	ZOW	1	0.83%
36	ZOP	1	0.83%
37	ZSZ	1	0.83%
38	ZUF	1	0.83%
39	ZWS	1	0.83%
40	ZWY	1	0.83%
41	ZWP	1	0.83%
42	ZVU	1	0.83%
43	ZUH	1	0.83%
44	YMX	1	0.83%
45	YEP	1	0.83%
46	WPF	1	0.83%
47	WSF	1	0.83%
48	VUO	1	0.83%
49	PYE	1	0.83%
50	VSG	1	0.83%

Cipher	plain
p	e
Z	t

cipher	plain
th	ZW
it	UZ

cipher	plain
the	ZWP
but	

1	HMD	2	1.67%
2	DZS	2	1.67%
3	ZHM	2	1.67%
4	PZH	1	0.83%
5	UEP	1	0.83%
6	UDT	1	0.83%
7	UDB	1	0.83%
8	TSX	1	0.83%
9	UFP	1	0.83%
10	UHS	1	0.83%
11	UZU	1	0.83%
12	UZW	1	0.83%
13	UZQ	1	0.83%
14	UPZ	1	0.83%
15	UOH	1	0.83%
16	TSV	1	0.83%
17	TMO	1	0.83%
18	SOV	1	0.83%
19	QSO	1	0.83%
20	SHZ	1	0.83%
21	SGZ	1	0.83%
22	SFP	1	0.83%
23	SVP	1	0.83%
24	SXA	1	0.83%
25	VGP	1	0.83%

26	SZU	1	0.83%
27	SZO	1	0.83%
28	SXU	1	0.83%
29	SXE	1	0.83%
30	QUZ	1	0.83%
31	VUE	1	0.83%
32	ZQS	1	0.83%
33	ZSH	1	0.83%
34	ZPE	1	0.83%
35	ZOW	1	0.83%
36	ZOP	1	0.83%
37	ZSZ	1	0.83%
38	ZUF	1	0.83%
39	ZWS	1	0.83%
40	ZWY	1	0.83%
41	ZWP	1	0.83%
42	ZVU	1	0.83%
43	ZUH	1	0.83%
44	YMX	1	0.83%
45	YEP	1	0.83%
46	WPF	1	0.83%
47	WSF	1	0.83%
48	VUO	1	0.83%
49	PYE	1	0.83%
50	VSG	1	0.83%

- guess P & 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
```

Affine Cipher

- Encryption

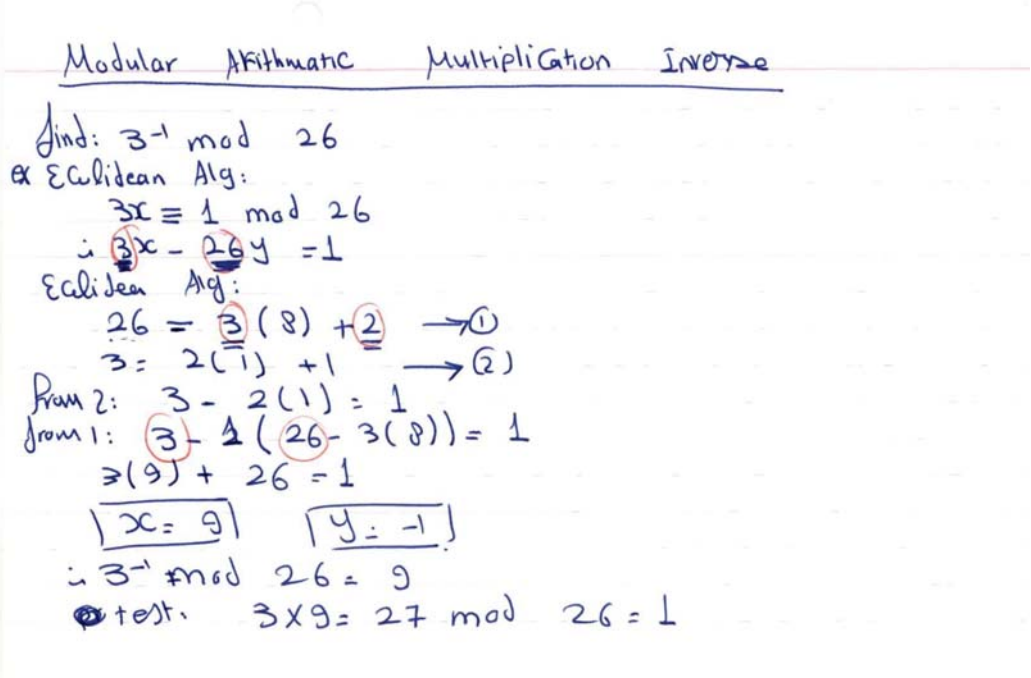
$$C = (a \times P + b) \bmod 26$$

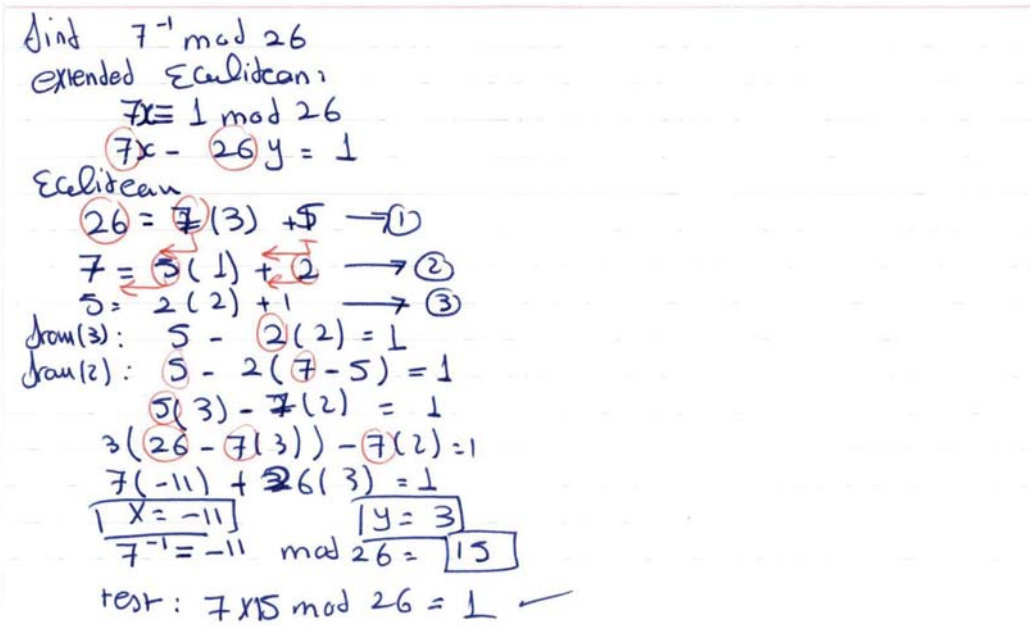
- Decryption

$$P = (c - b) \times a^{-1} \bmod 26$$

- Condition: gcd(a,26) = 1 ; or a^{-1} is an inverse of a modulo 26

Modular multiplicative inverse



- 

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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	d	f	h	j	l	p	r	t	v	x	z
1	3	5	7	9	11	15	17	19	21	23	25

1	9	21	15	3	19	7	23	11	5	17	25
b	j	v	p	d	t	h	x	l	f	r	z

Cryptanalysis

- Brute force attack = total number of possible values for *a* × total number of possible values for *b*
- *= 26*12 = 312 possible keys*

- Example
- Using affine cipher, encrypt the following message

  “sent you a cheque waiting your feedback”
- Using the following keys

a=f,

b=v

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

plaintext

s	e	n	t	y	o	U	a	c	h	e	q	u	e	w	a	i	t	i	n	g	y	o	u	r	f	e	e	d	b	a	c	K
18	4	13	9	4	4	0	0	2	7	4	6	0	4	2	0	8	9	8	3	6	4	4	0	7	5	4	4	3	1	0	2	0

a	b
F	v
5	21

ciphertext

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

plaintext

s	e	n	t	y	o	U	a	c	h	e	q	u	e	w	a	i	t	i	n	g	y	o	u	r	f	e	e	d	b	a	c	K
18	4	13	9	4	4	0	0	2	7	4	6	0	4	2	0	8	9	8	3	6	4	4	0	7	5	4	4	3	1	0	2	0

a	b
F	v
5	21

ciphertext

17	5	8	2	1	3	7	1	5	4	5	3	7	5	1	1	9	2	9	8	5	1	3	7	2	0	5	5	0	0	1	5	9
h	p	i	ml	n	r	v	f	e	p	x	r	p	b	v	j	mj	i	z	l	n	r	c	u	p	p	k	a	v	f	t		

Using affine cipher, decrypt the following received message

“cpfjpwpkinmejizfepftlnrcavit”

Using same keys

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

ciphertext

c	p	f	j	p	w	p	k	i	n	m	e	j	i	z	f	e	p	f	t	l	n	r	c	a	v	i	T
2	15	5	9	15	22	15	10	8	13	12	4	9	8	25	5	4	15	5	19	11	13	17	2	0	21	8	19

a	a^{-1}	b
F	V	v
5	21	21

plaintext

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

ciphertext

c	p	f	j	p	w	p	k	i	n	m	e	j	i	z	f	e	p	f	t	l	n	r	c	a	v	i	T
2	15	5	9	15	22	15	10	8	13	12	4	9	8	25	5	4	15	5	19	11	13	17	2	0	21	8	19

a	a^{-1}	b
F	V	v
5	21	21

plaintext

17	4	2	8	4	21	4	3	13	14	19	7	8	13	6	2	7	4	2	10	24	14	20	17	1	0	13	10
r	e	c	i	e	v	e	d	n	o	t	h	i	n	g	c	h	e	c	k	y	o	u	r	b	a	n	k

Thanks,..

See you next week (ISA),…