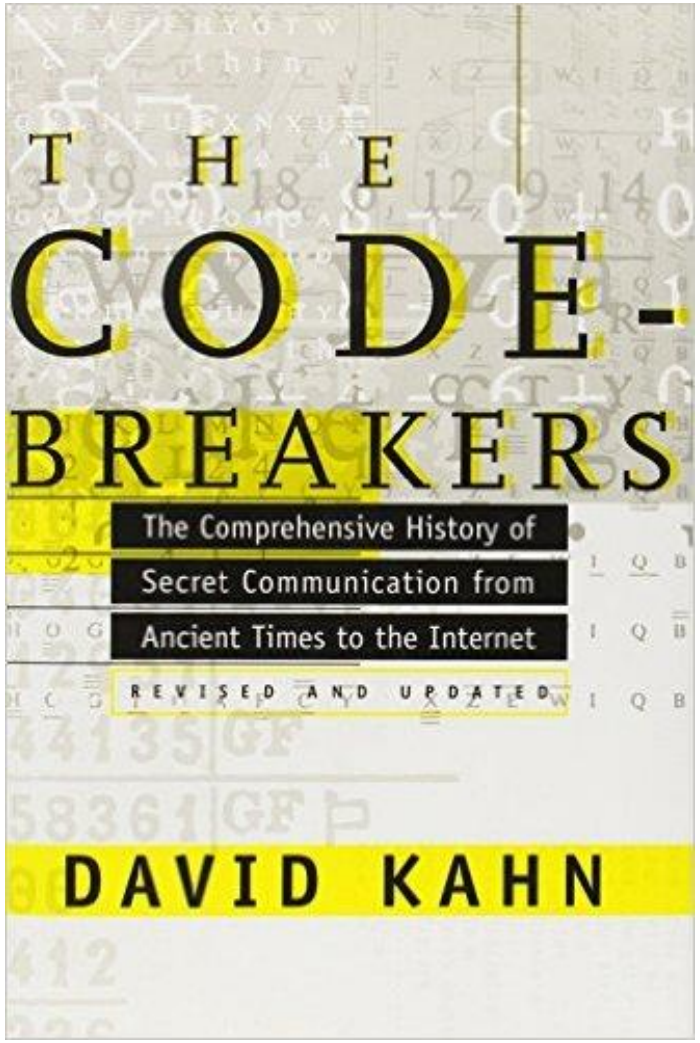
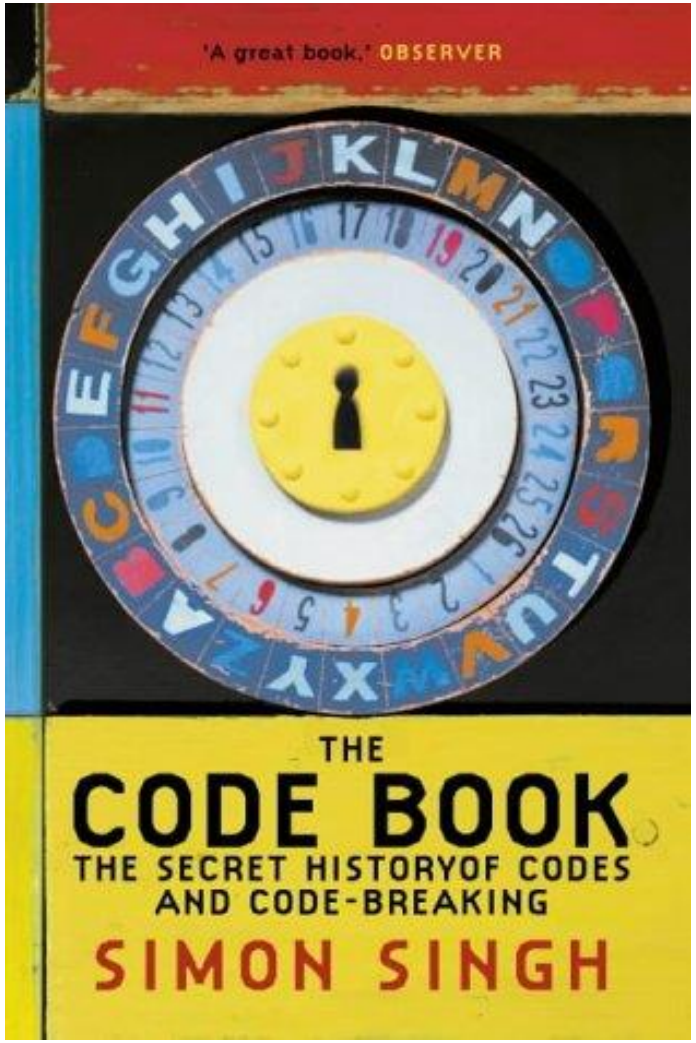
Cryptanalysis

A walk through time

Arka Rai Choudhuri

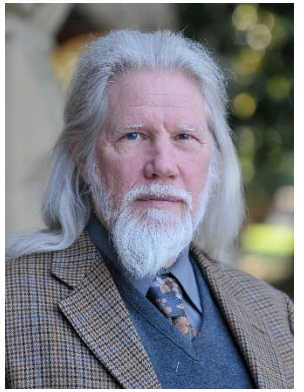
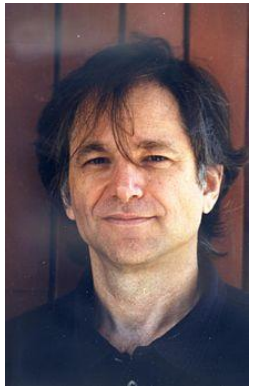
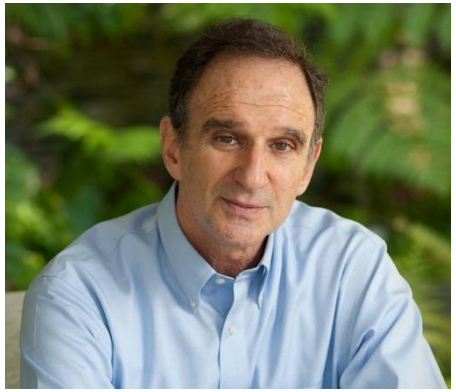
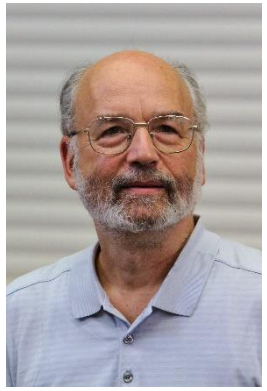
arkarai.choudhuri@gmail.com

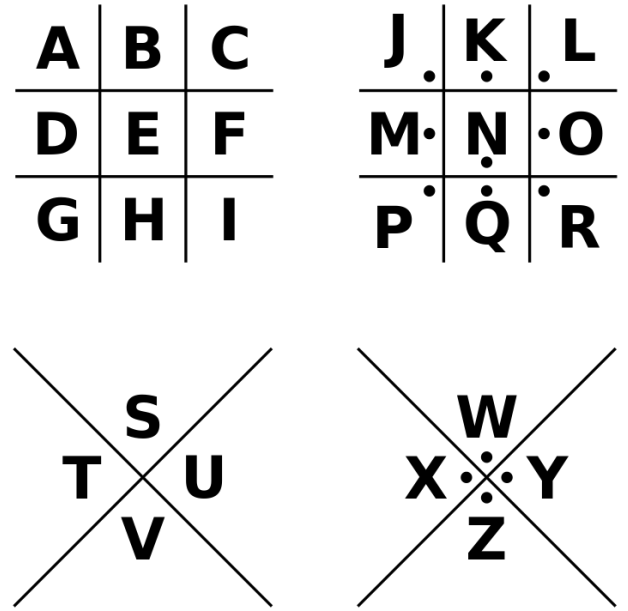

THE
CODE-
BREAKERS
The Comprehensive History of
Secret Communication from
Ancient Times to the Internet
REVISED AND UPDATED
DAVID KAHN


'A great book.' OBSERVER
THE
CODE BOOK
THE SECRET HISTORYOF CODES
AND CODE-BREAKING
SIMON SINGH

How many can you identify?



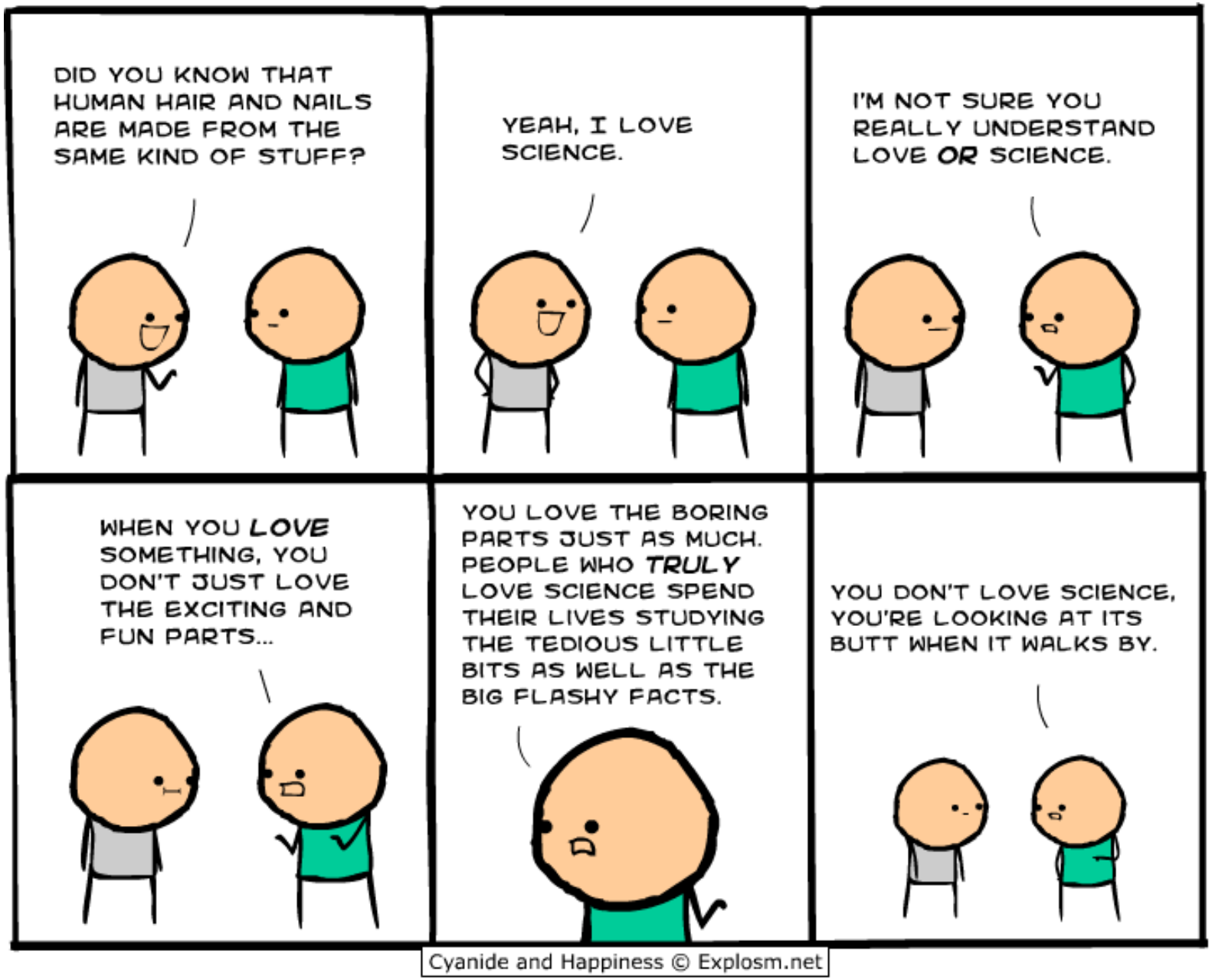



History

(or how I will give you hope of becoming world famous and earning $70 million along the way)

Disclaimer

Cryptography's butt



http://explosm.net/comics/3557/

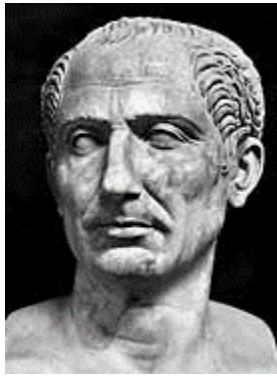
AOUSATUPRSVNEG

SOURAV SEN GUPTA

USVRAO ENS PUTGA

Transposition Cipher

Caesar cipher



Simple shifting of letters.

Plain alphabet	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
Cipher alphabet	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

Only 13 possible keys.

Easy to break exhaustively.

Substitution Cipher

Earliest mention in the Kama-sutra.

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

26! Number of keys.

403 291 461 126 605 635 584 000 000

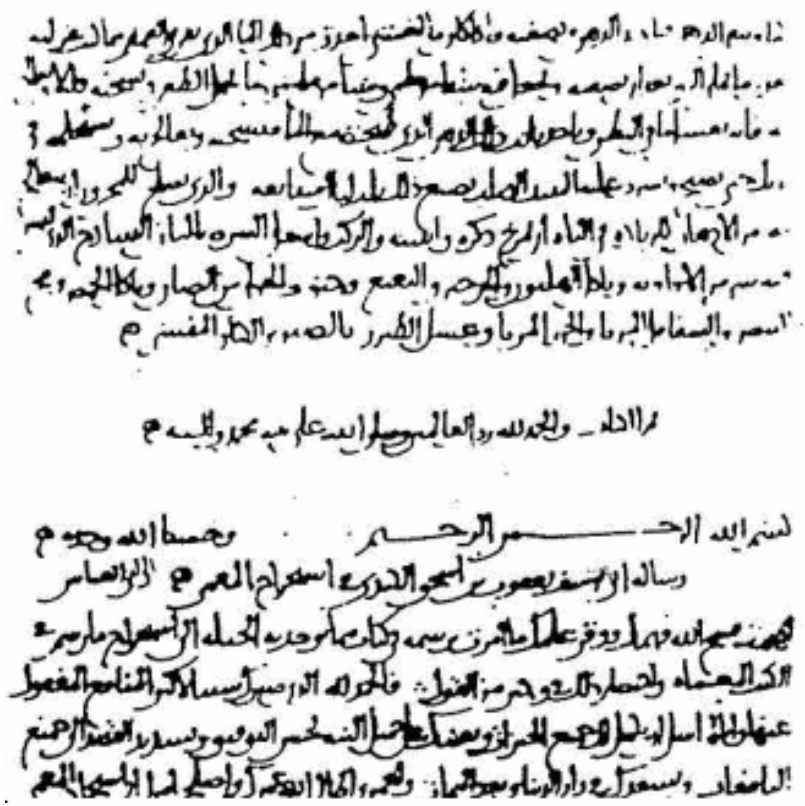
88 bits of secrecy.

Arab Cryptanalysis

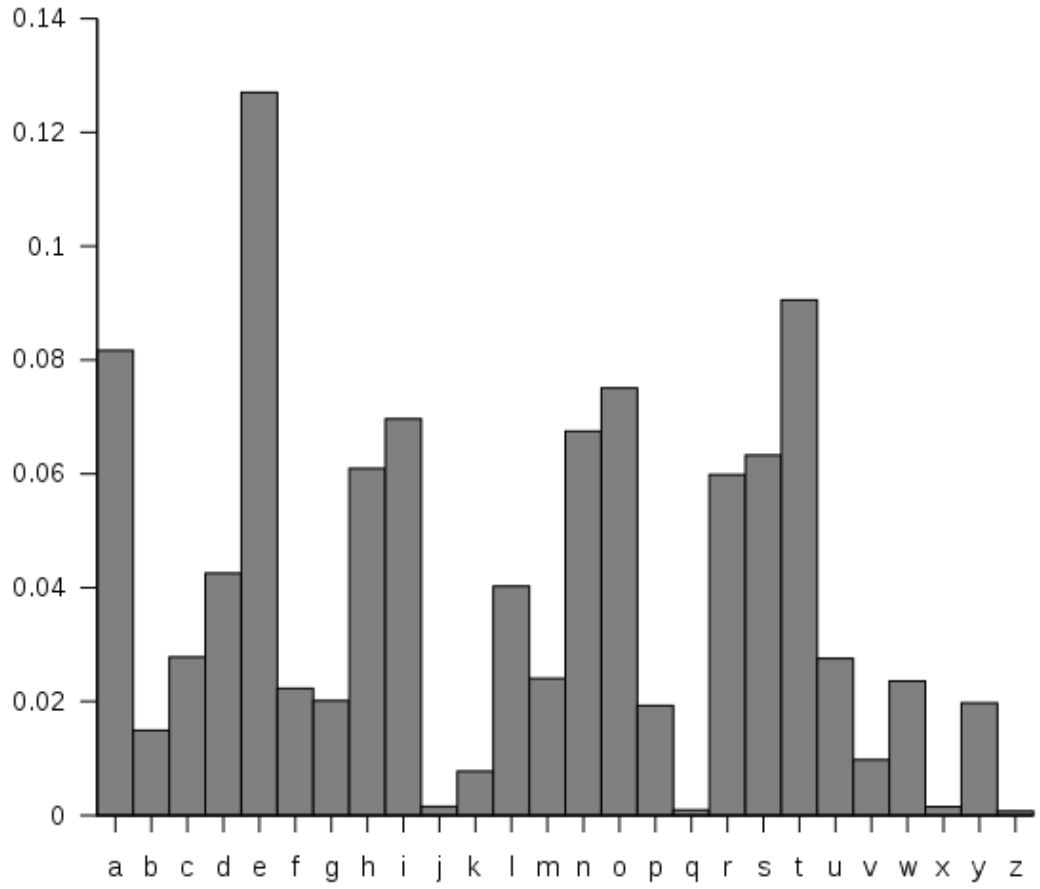
Al-Kindi “On Deciphering Cryptographic Messages”

9th century

FREQUENY ANALYSIS



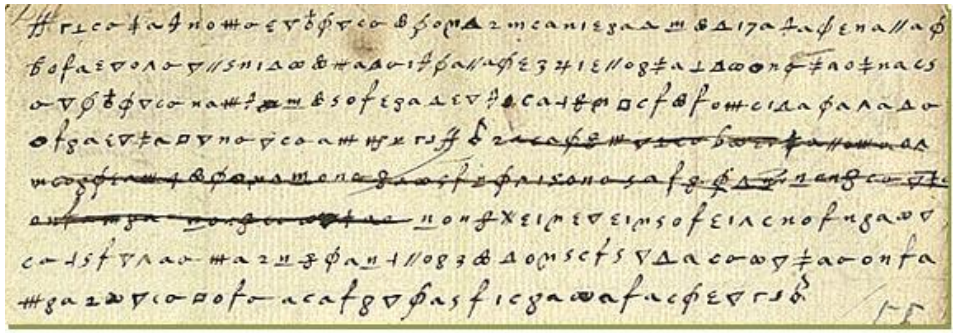
Structure of the English language

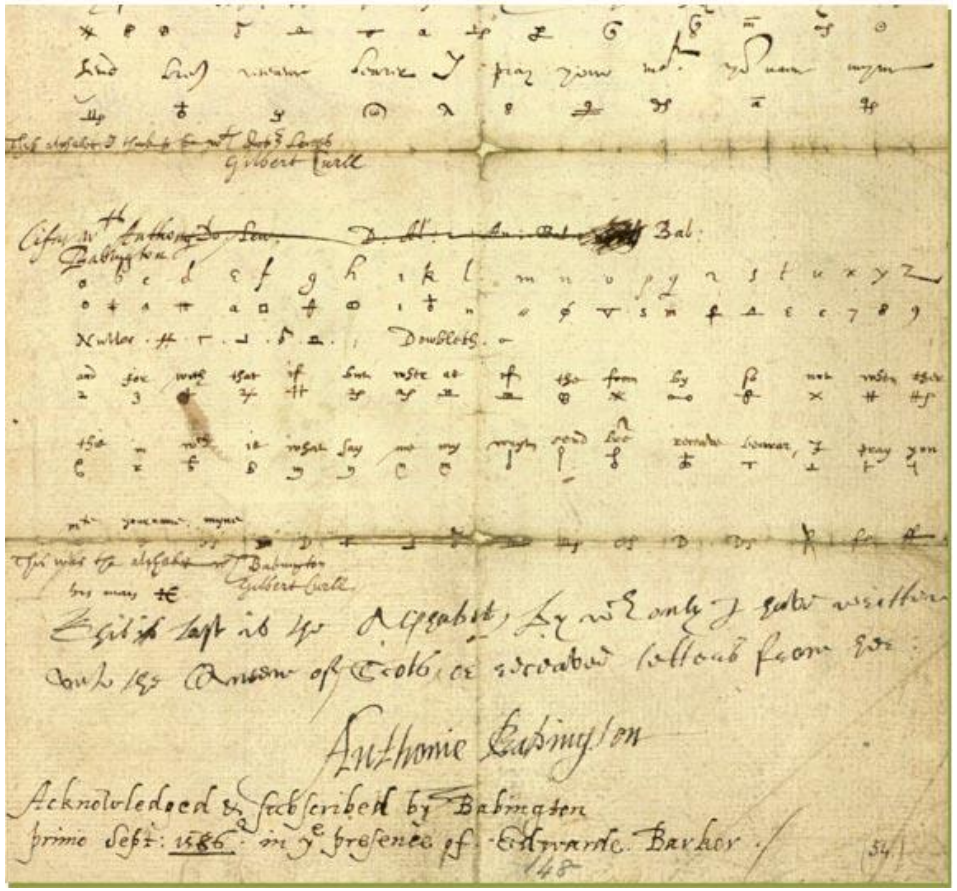


Move to digrams and trigrams for better results.

Mary Queen of Scots (16th Century)

Assassinate





Solved by Elizabeth's cryptanalyst


J.F.Rigaud RA Pinx.
W.N.Gardiner Sc.
The Queen, laying herself down on the Ground, and stretching forth her Neck on the Block, repeats many times, "Into thy Hands, O Lord I do commit my Spirit."
gettyimages
Hulton Archive
51244575

Vigenère cipher (16th century)

Overcome the statistical weakness of ciphers?

Polyalphabetic ciphers

- A letter in the cipher can represent multiple letters from the plain text

Not broken till the 19th century.

Keyword	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I
Plaintext	d	i	v	e	r	t	t	r	o	o	p	s	t	o	e	a	s	t	r	i	d	g	e
Ciphertext	Z	P	D	X	V	P	A	Z	H	S	L	Z	B	H	I	W	Z	B	K	M	Z	N	M

How do we figure out the length?

Use properties of the English language.

$$\sum_{i=0}^{25} p_i^2 \approx 0.065$$

If p_i follow the letter frequencies. Else,

$$\sum_{i=0}^{25} \frac{1}{26^2} \approx 0.038$$

Increase the keyword length?

Create a keyword that is as long as the message.

Can’t use the methods discussed previously.

Are we done?

Key	? ?
Plaintext	? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N ? ? ? B S J ? ? ? ? ? Y P T ? ? ? ?
Plaintext	t h e ? ? ? t h e ? ? ? ? ? t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N ? ? ? ? ? A P O C A L Y P T I C ? ?
Plaintext	t h e ? ? ? ? ? n q c b e o t h e x g ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N ? ? ? ? ? ? ? ? ? C R Y P T ? ? ? ?
Plaintext	t h e ? ? ? ? ? ? ? ? ? c i t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N ? ? ? ? ? ? ? ? ? E G Y P T ? ? ? ?
Plaintext	t h e ? ? ? ? ? ? ? ? ? a t t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N A D A ? ? ? ? ? ? E G Y P T ? ? ? ?
Plaintext	t h e m e e ? ? ? ? ? ? a t t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

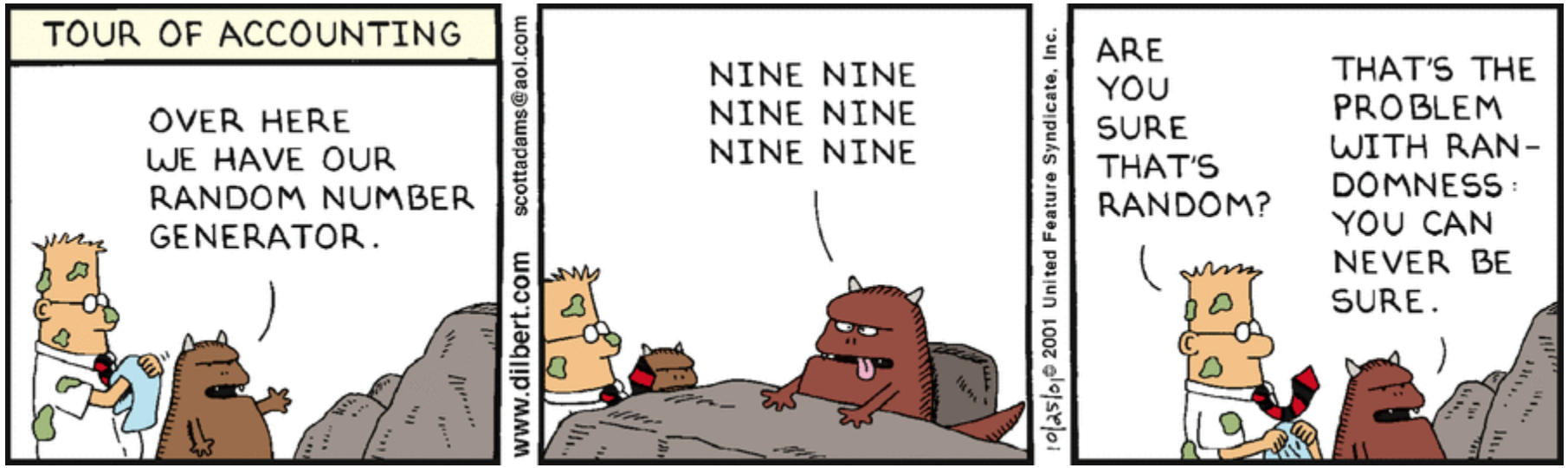
Key	C A N A D A B R A Z I L E G Y P T C U B A
Plaintext	t h e m e e t i n g i s a t t h e d o c k
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Failed because the key wasn't "random" enough?

What is random?

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

https://xkcd.com/221/



http://dilbert.com/strip/2001-10-25

Why does it work?

Key	P L M O E Z Q K J Z L R T E A V C R C B Y
Plaintext	a t t a c k t h e v a l l e y a t d a w n
Ciphertext	P E F O G J J R N U L C E I Y V V U C X L

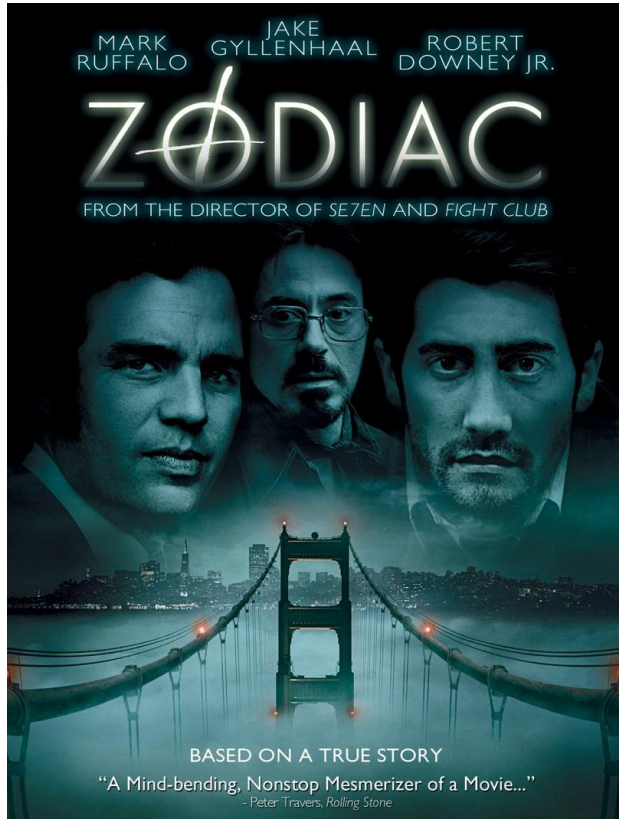
Key	M A A K T G Q K J N D R T I F D B H K T S
Plaintext	d e f e n d t h e h i l l a t s u n s e t
Ciphertext	P E F O G J J R N U L C E I Y V V U C X L

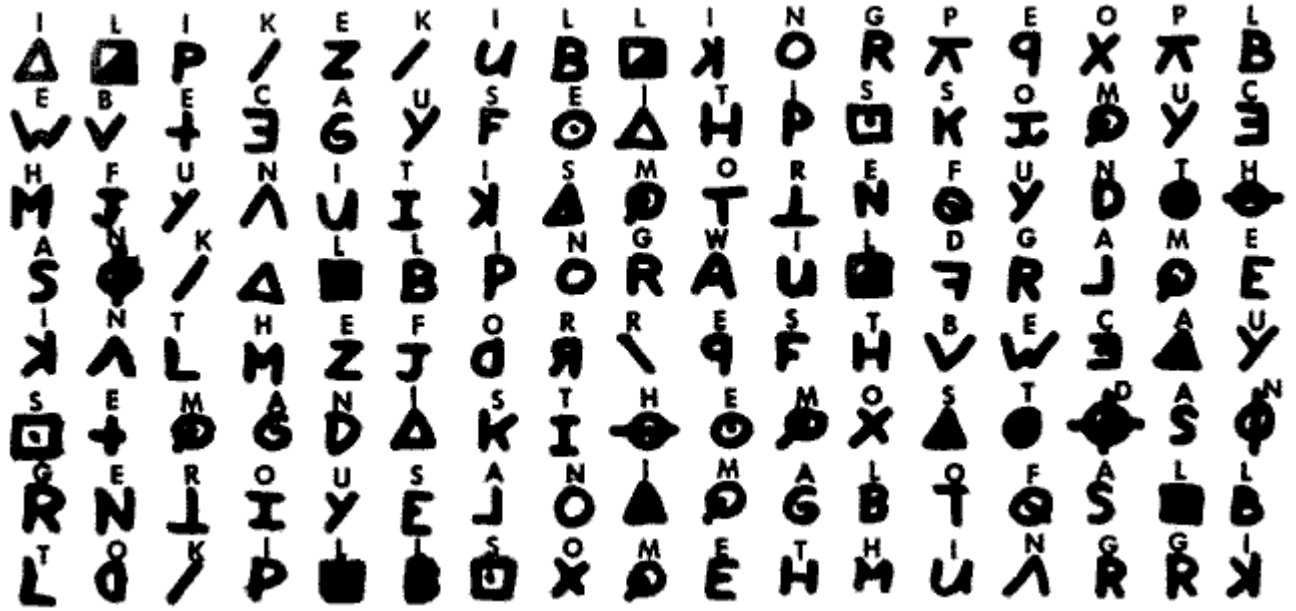
Generate all possible plaintexts from a given ciphertext.
All the keys will look random.

Zodiac

Late 60s in the US.

Killer sent ciphers to solve.

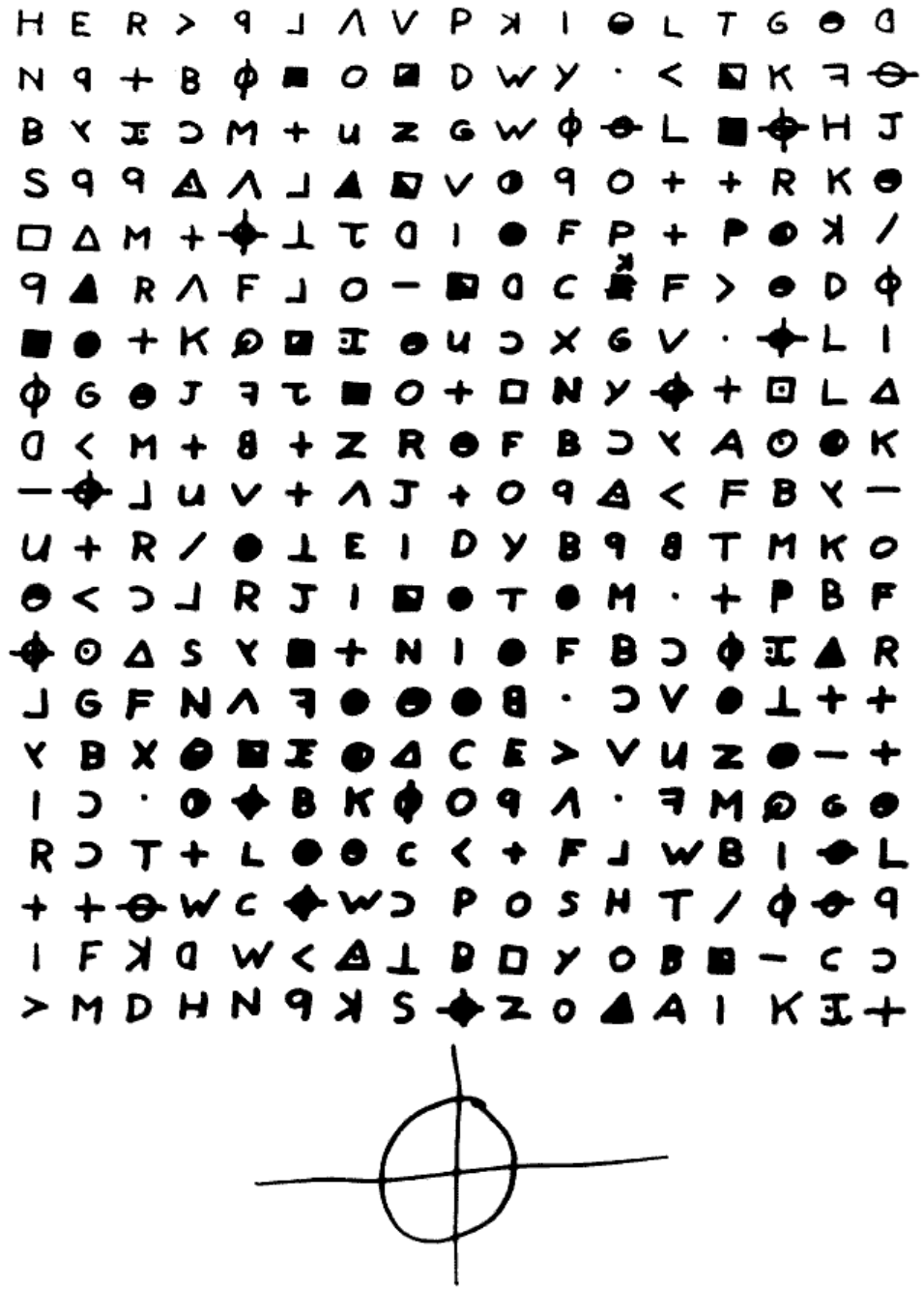




“I LIKE KILLING PEOPLE BECAUSE IT IS SO MUCH FUN IT IS MORE FUN THAN KILLING WILD GAME IN THE FORREST BECAUSE MAN IS THE MOST DANGEROUE ANAMAL OF ALL TO KILL SOMETHING GI..”

But who is the zodiac?

340 character cipher.
Unsolved to this day.

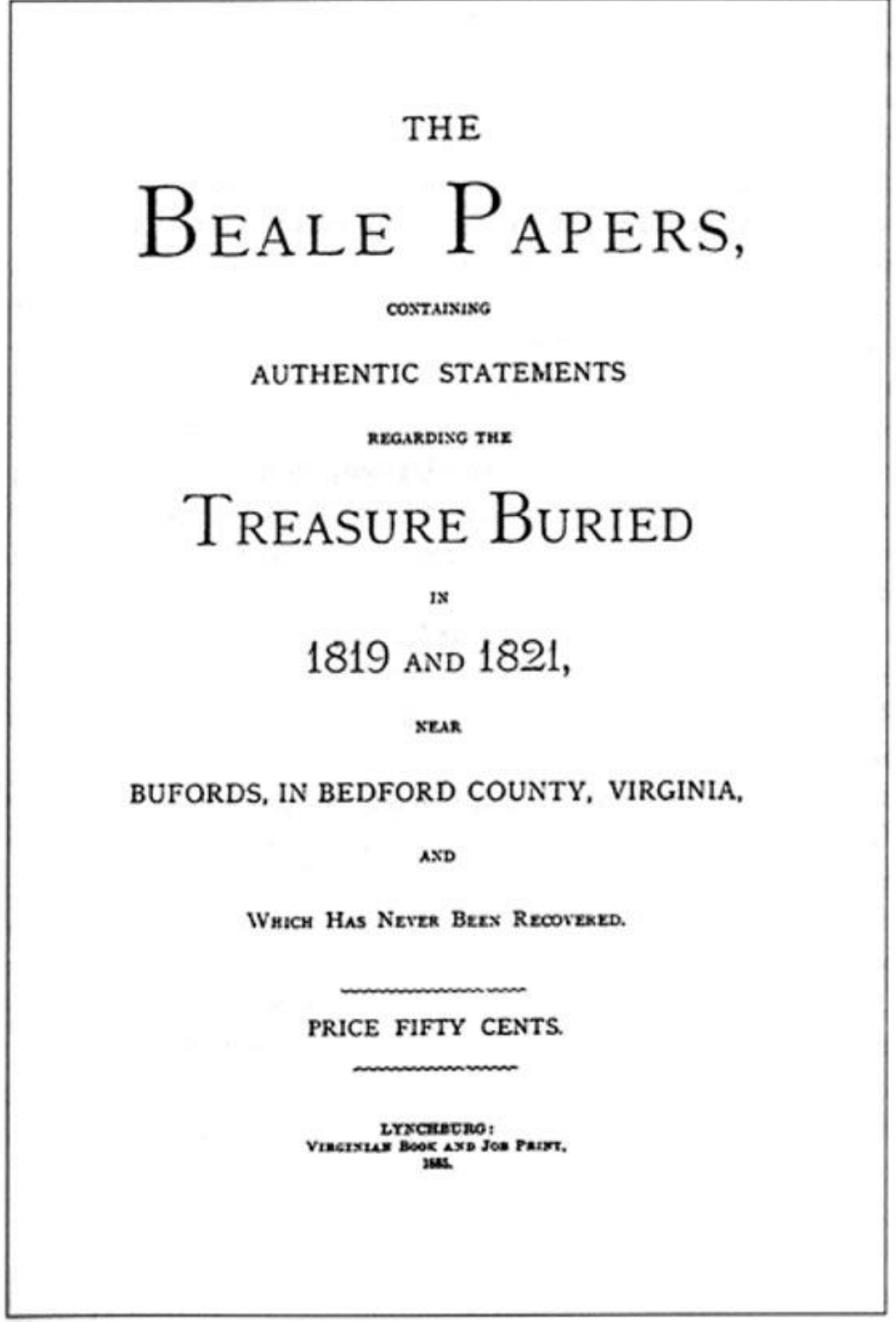


This is the Zodiac speaking
By the way have you cracked
the last cipher I sent you ?.
My name is ——

A E N ⊕ ⊗ K ⊗ M ⊗ ⊔ N A M

I am mildly cerous as to how
much money you have on my
head now. I hope you do not
think that I was the one
who wiped out that blue
meannie with a bomb at the
cop station. Even though I talked
about killing school children with
one. It just wouldnt do to
move in on someone elses territory.
But there is more glory in killing
a cop than a cid because a cop
can shoot back. I have killed
ten people to date. It would
have been a lot more except
that my bas bomb was a dud.
I was swamped out by the
rain we had a while back.

Beale cipher



THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
1885.

3 cipher

- Location
- Contents
- Names of treasure owners

3 cipher

- Location
- Contents
- Names of treasure owners

Buried treasure of gold, silver and jewels estimated to be worth over US$63 million as of September 2011

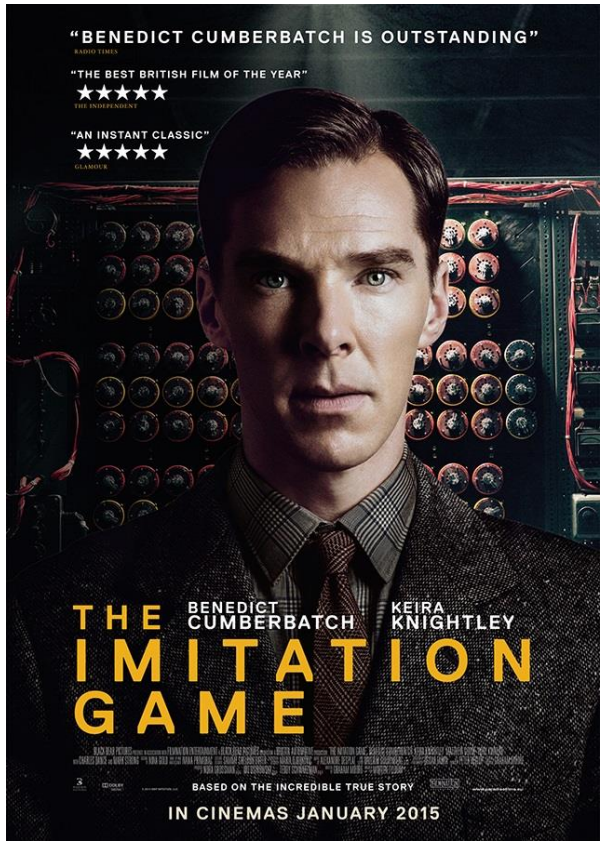
115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

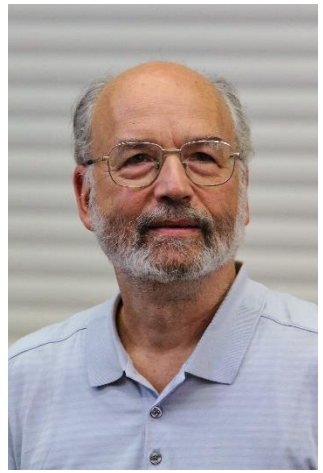
Was it an elaborate hoax?

Why has it withstood cryptanalysis for centuries?

Enigma

Marian Rejewski

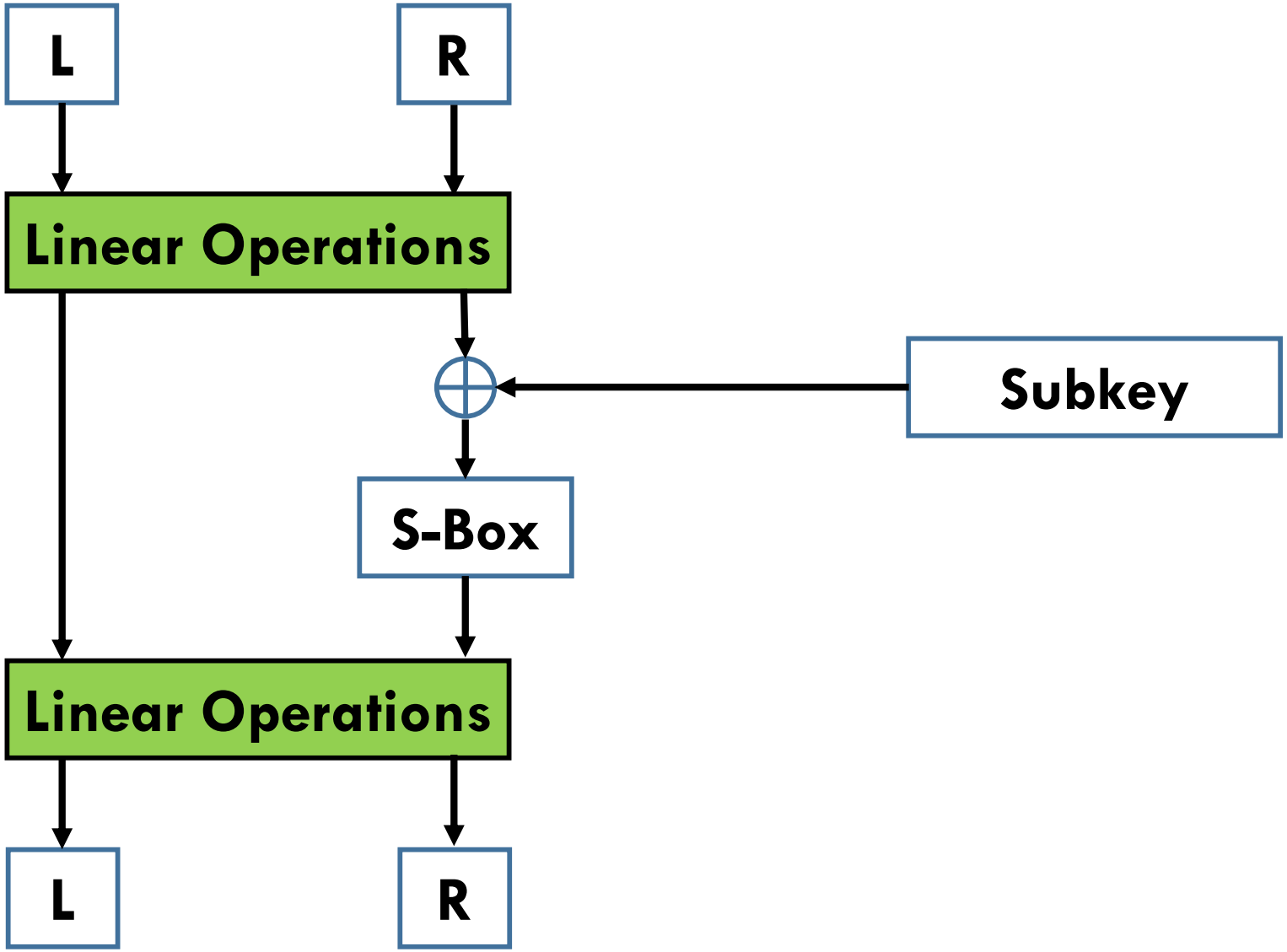




Differential Cryptanalysis

Where your disillusionment dies.

DES



S-Box

Substitution boxes

Non-Linear

Can’t represent output bits as linear operation of input bits.

S-Box

Substitution boxes

Non-Linear

Implemented by a table look-up

S-Box

S1(101011)

S1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

S2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
1	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
2	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
3	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9

S3

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
1	D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
2	D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
3	1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C

S4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
1	D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
2	A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3	3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E

S5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
1	E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
2	4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
3	B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3

S6

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
1	A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
2	9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
3	4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D

S7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
1	D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
2	1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
3	6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C

S8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1	1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
2	7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
3	2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

S-Box

S1(101011)

S1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

S2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
1	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
2	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
3	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9

S3

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
1	D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
2	D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
3	1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C

S4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
1	D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
2	A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3	3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E

S5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
1	E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
2	4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
3	B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3

S6

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
1	A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
2	9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
3	4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D

S7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
1	D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
2	1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
3	6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C

S8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1	1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
2	7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
3	2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

S-Box

$S1(101011) = 7$

S1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

S2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
1	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
2	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
3	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9

S3

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
1	D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
2	D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
3	1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C

S4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
1	D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
2	A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3	3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E

S5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
1	E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
2	4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
3	B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3

S6

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
1	A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
2	9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
3	4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D

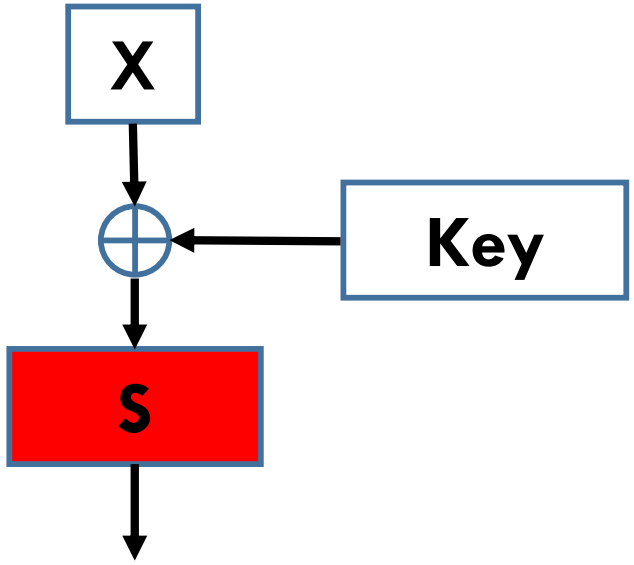
S7

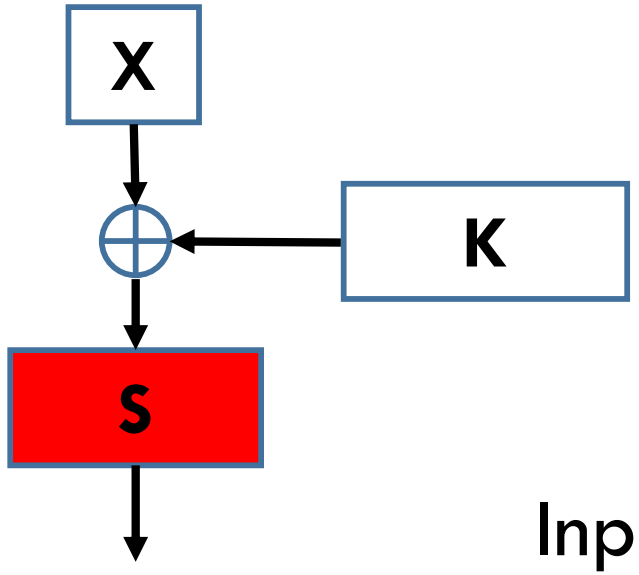
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
1	D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
2	1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
3	6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C

S8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1	1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
2	7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
3	2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

How can we use an S-box?





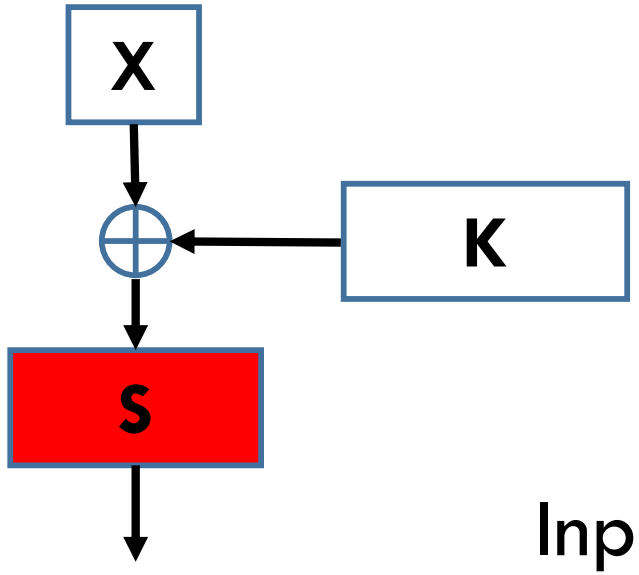
	00	01	10	11
0	10	01	11	00
1	00	10	01	11

Inputs are known

$$X_1 = 110 \; and \; X_2 = 010$$

Outputs of S-box known

$$S(X_1 \oplus K) = 10 \; and \; S(X_2 \oplus K\,) = 01$$



	00	01	10	11
0	10	01	11	00
1	00	10	01	11

Inputs are known

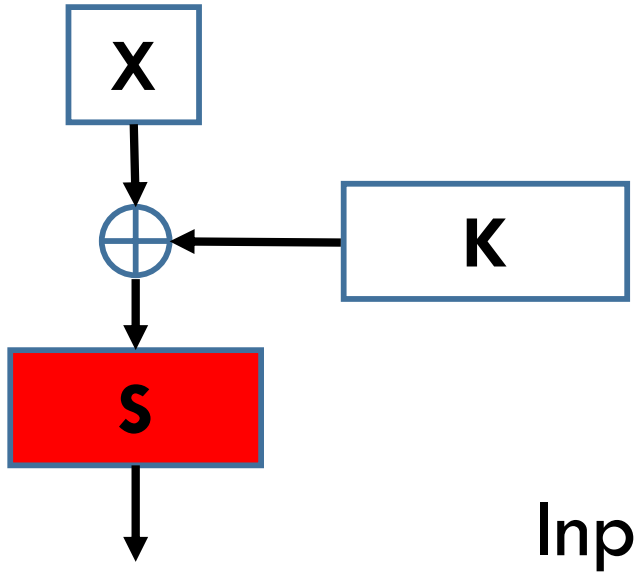
$$X_1 = 110 \; and \; X_2 = 010$$

Outputs of S-box known

$$S(X_1 \oplus K) = 10 \; and \; S(X_2 \oplus K\,) = 01$$

$$X_1 \oplus K \in \{000,101\}$$

$$\Longrightarrow K \in \{110,011\}$$



	00	01	10	11
0	10	01	11	00
1	00	10	01	11

Inputs are known

$$X_1 = 110 \; and \; X_2 = 010$$

Outputs of S-box known

$$S(X_1 \oplus K) = 10 \; and \; S(X_2 \oplus K\,) = 01$$

$X_1 \oplus K \in \{000,101\}$
$\Longrightarrow K \in \{110,011\}$

K=011

$X_2 \oplus K \in \{001,110\}$
$\Longrightarrow K \in \{011,100\}$

Differences

Focus on input and output differences.

We know the inputs X_1 and X_2. But the input to the S-boxes are $X_1 \oplus K$ and $X_2 \oplus K$.

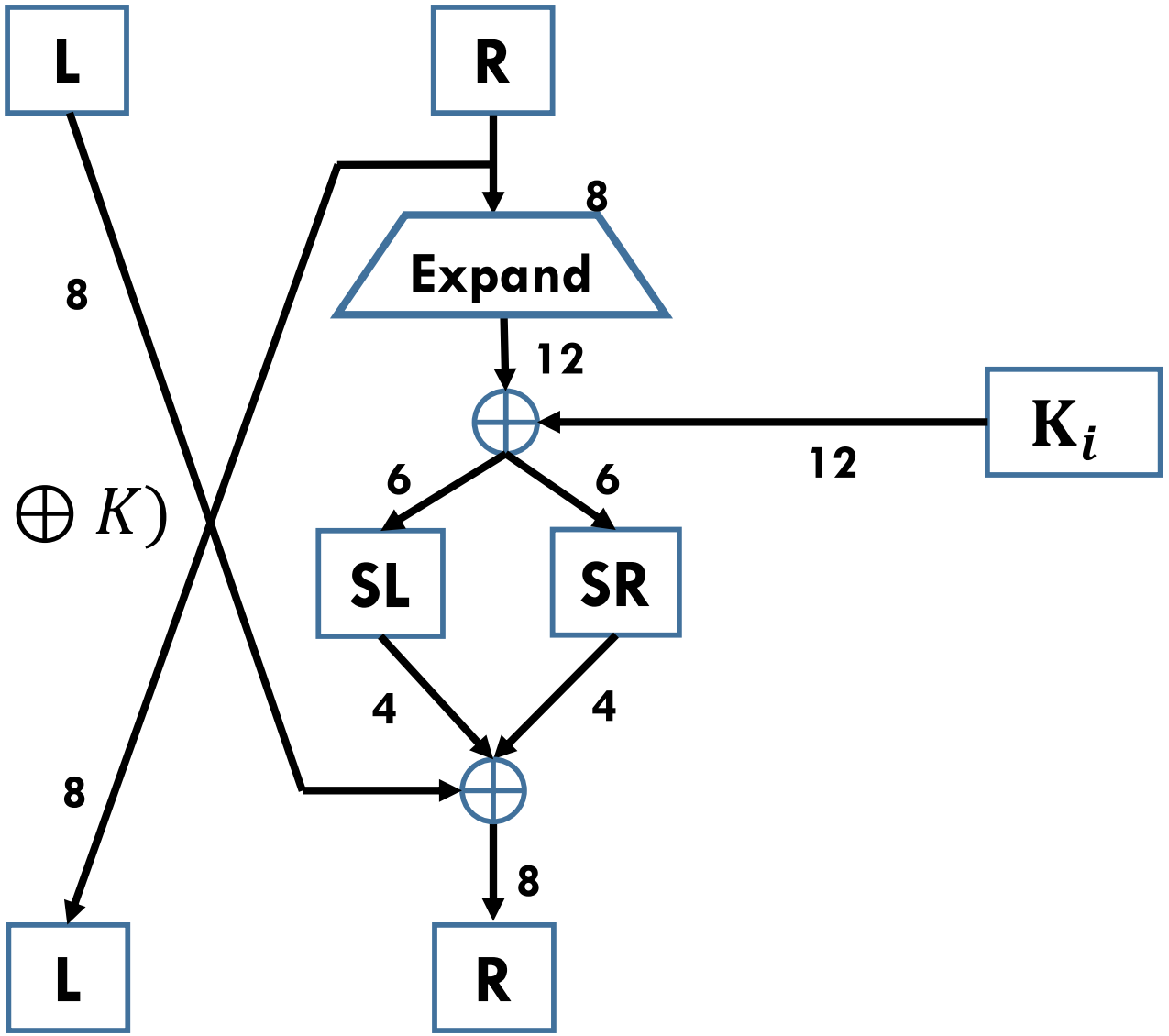
XOR of the input to the S-box

$$(X_1 \oplus K) \oplus (X_2 \oplus K) = X_1 \oplus X_2$$

The difference is independent of the key.

TINY DES (TDES)

$$F(R, K) = S(expand(R) \oplus K)$$



x_0x_5	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	5	0	A	E	7	2	8	D	4	3	9	6	F	1	B
1	1	C	9	6	3	E	B	2	F	8	4	5	D	A	0	7
2	F	A	E	6	D	8	2	4	1	7	9	0	3	5	B	C
3	0	A	3	C	8	2	1	E	9	7	F	6	B	5	D	4

$$K_1 = k_2k_4k_5k_6k_7k_1k_{10}k_{11}k_{12}k_{14}k_{15}k_8$$
$$K_2 = k_4k_6k_7k_0k_1k_3k_{11}k_{12}k_{13}k_{15}k_8k_9$$
$$K_3 = k_6k_0k_1k_2k_3k_5k_{12}k_{13}k_{14}k_8k_9k_{10}$$
$$K_4 = k_0k_2k_3k_4k_5k_7k_{13}k_{14}k_{15}k_9k_{10}k_{11}$$

x_0x_5	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	5	0	A	E	7	2	8	D	4	3	9	6	F	1	B
1	1	C	9	6	3	E	B	2	F	8	4	5	D	A	0	7
2	F	A	E	6	D	8	2	4	1	7	9	0	3	5	B	C
3	0	A	3	C	8	2	1	E	9	7	F	6	B	5	D	4

$$K_1 = k_2k_4k_5k_6k_7k_1k_{10}k_{11}k_{12}k_{14}k_{15}k_8$$
$$K_2 = k_4k_6k_7k_0k_1k_3k_{11}k_{12}k_{13}k_{15}k_8k_9$$
$$K_3 = k_6k_0k_1k_2k_3k_5k_{12}k_{13}k_{14}k_8k_9k_{10}$$
$$K_4 = k_0k_2k_3k_4k_5k_7k_{13}k_{14}k_{15}k_9k_{10}k_{11}$$

$$expand(R) = expand(r_0r_1 \cdots r_7) = (r_4r_7r_2r_1r_5r_7r_0r_2r_6r_5r_0r_3)$$

$X_1 \oplus X_2 = 001000 \Longrightarrow SR(X_1) \oplus SR(X_2) = 0010$ with probability ¾

If $X_1 \oplus X_2 = 000000 \Longrightarrow SR(X_1) \oplus SR(X_2) = 0000$ with probability 1

Chosen plaintext attack

$$P = (L_0||R_0)\ and\ \tilde{P} = (\widetilde{L_0}||\widetilde{R_0})$$

$$P \oplus \tilde{P} = (L_0||R_0) \oplus (\tilde{L}_0||\widetilde{R_0}) = 0000\ 0000\ 0000\ 0010 = 0x0002$$

Is the “expand” function linear?

$$expand(X_1) \oplus expand(X_1) = expand(X_1 \oplus X_2)$$

$$R_0 \oplus \tilde{R}_0 = 0000\ 0010 \Longrightarrow expand(R_0) \oplus expand\left(\tilde{R}_0\right) = expand\left(R_0 \oplus \tilde{R}_0\right)$$
$$= expand(0000\ 0010)$$
$$= 000000\ 001000$$

$$F(R_0, K) \oplus F\left(\widetilde{R_0}, K\right) = S(e(R_0) \oplus K) \oplus S(e\left(\tilde{R}_0\right) \oplus K)$$
$$= 0000\ 0010 \text{ with probability } ¾$$

$$
\begin{aligned}
R_2 \oplus \widetilde{R_2} &= \left(L_1 \oplus F(R_1, K_2)\right) \oplus (\tilde{L}_1 \oplus F(\tilde{R}_1, K_2)) \\
&= \left(L_1 \oplus \tilde{L}_1\right) \oplus (F(R_1, K_2) \oplus F(\tilde{R}_1, K_2)) \\
&= \left(R_0 \oplus \tilde{R}_0\right) \oplus (F(R_1, K_2) \oplus F(\tilde{R}_1, K_2)) \\
&= 0000\ 0010 \oplus 0000\ 0010 \\
&= 0000\ 0000
\end{aligned}
$$

With probability $\frac{3}{4} \times \frac{3}{4}$

$(L_0 \| R_0) = P$	$(\tilde{L}_0 \| \tilde{R}_0) = \tilde{P}$	$P \oplus \tilde{P} = \texttt{0x0002}$	Probability
$L_1 = R_0$	$\tilde{L}_1 = \tilde{R}_0$		
$R_1 = L_0 \oplus F(R_0, K_1)$	$\tilde{R}_1 = \tilde{L}_0 \oplus F(\tilde{R}_0, K_1)$	$(L_1 \| R_1) \oplus (\tilde{L}_1 \| \tilde{R}_1) = \texttt{0x0202}$	$3/4$
$L_2 = R_1$	$\tilde{L}_2 = \tilde{R}_1$		
$R_2 = L_1 \oplus F(R_1, K_2)$	$\tilde{R}_2 = \tilde{L}_1 \oplus F(\tilde{R}_1, K_2)$	$(L_2 \| R_2) \oplus (\tilde{L}_2 \| \tilde{R}_2) = \texttt{0x0200}$	$(3/4)^2$
$L_3 = R_2$	$\tilde{L}_3 = \tilde{R}_2$		
$R_3 = L_2 \oplus F(R_2, K_3)$	$\tilde{R}_3 = \tilde{L}_2 \oplus F(\tilde{R}_2, K_3)$	$(L_3 \| R_3) \oplus (\tilde{L}_3 \| \tilde{R}_3) = \texttt{0x0002}$	$(3/4)^2$
$L_4 = R_3$	$\tilde{L}_4 = \tilde{R}_3$		
$R_4 = L_3 \oplus F(R_3, K_4)$	$\tilde{R}_4 = \tilde{L}_3 \oplus F(\tilde{R}_3, K_4)$	$(L_4 \| R_4) \oplus (\tilde{L}_4 \| \tilde{R}_4) = \texttt{0x0202}$	$(3/4)^3$
$C = (L_4 \| R_4)$	$C = (\tilde{L}_4 \| \tilde{R}_4)$	$C \oplus \tilde{C} = \texttt{0x0202}$	

Recovering the key

What do we have?

$$P \oplus \tilde{P} \Longrightarrow (L_0 \oplus \tilde{L}_0) || (R_0 \oplus \tilde{R}_0)$$

$$C \oplus \tilde{C} \Longrightarrow (L_4 \oplus \tilde{L}_4) || (R_4 \oplus \tilde{R}_4)$$

$$R_4 = L_3 \oplus F(R_3, K_4) \; and \; \tilde{R}_4 = \tilde{L}_3 \oplus F\left(\tilde{R}_3, K_4\right)$$

$$\Longrightarrow R_4 = L_3 \oplus F(L_4, K_4) \; and \; \tilde{R}_4 = \tilde{L}_3 \oplus F\left(\tilde{L}_4, K_4\right)$$

$$\Longrightarrow L_3 = R_4 \oplus F(L_4, K_4) \; and \; \tilde{L}_3 = \tilde{R}_4 \oplus F\left(\tilde{L}_4, K_4\right)$$

If

$$C \oplus \tilde{C} = 0x0202,$$

with high probability,

$$L_3 = \tilde{L}_3$$
$$\Longrightarrow R_4 \oplus F(L_4, K_4) = \tilde{R}_4 \oplus F\left(\tilde{L}_4, K_4\right)$$
$$\Longrightarrow R_4 \oplus \tilde{R}_4 = F(L_4, K_4) \oplus F\left(\tilde{L}_4, K_4\right)$$

If

$$C \oplus \tilde{C} = 0x0202,$$

with high probability,

$$L_3 = \tilde{L}_3$$
$$\Longrightarrow R_4 \oplus F(L_4, K_4) = \tilde{R}_4 \oplus F\left(\tilde{L}_4, K_4\right)$$
$$\Longrightarrow R_4 \oplus \tilde{R}_4 = F(L_4, K_4) \oplus F\left(\tilde{L}_4, K_4\right)$$

Let,

$$L_4 = l_0 l_1 l_2 l_3 l_4 l_5 l_6 l_7 \; and \; \tilde{L}_4 = \tilde{l}_0 \tilde{l}_1 \tilde{l}_2 \tilde{l}_3 \tilde{l}_4 \tilde{l}_5 \tilde{l}_6 \tilde{l}_7$$

Then

$$0000\ 0010 = (SL(l_4 l_7 l_2 l_1 l_5 l_7 \oplus k_0 k_2 k_3 k_4 k_5 k_7) || SR(l_0 l_2 l_6 l_5 l_0 l_3 \oplus k_{13} k_{14} k_{15} k_9 k_{10} k_{11}))$$
$$\oplus (SL(\tilde{l}_4 \tilde{l}_7 \tilde{l}_2 \tilde{l}_1 \tilde{l}_5 \tilde{l}_7 \oplus k_0 k_2 k_3 k_4 k_5 k_7) || SR(\tilde{l}_0 \tilde{l}_2 \tilde{l}_6 \tilde{l}_5 \tilde{l}_0 \tilde{l}_3 \oplus k_{13} k_{14} k_{15} k_9 k_{10} k_{11}))$$

Algorithm

1. Pick plaintext pairs with the given difference.
2. Run the algorithm with the unknown key to get ciphertext pairs.
3. Discard ciphertext pairs that don't satisfy output difference.
4. For all possible values of the 6 key bits identified, check if the derived condition holds.

count[i] = 0, for $i = 0, 1, \ldots, 63$
for $i = 1$ to iterations
    Choose P and $\tilde{P}$ with $P \oplus \tilde{P} =$ 0x0002
    Obtain corresponding $C = c_0 c_1 \ldots c_{15}$ and $\tilde{C} = \tilde{c}_0 \tilde{c}_1 \ldots \tilde{c}_{15}$
    if $C \oplus \tilde{C} =$ 0x0202 then
        $\ell_i = c_i$ and $\tilde{\ell}_i = \tilde{c}_i$ for $i = 0, 1, \ldots, 7$
        for $K = 0$ to 63
            if 0010 == (SboxRight($\ell_0 \ell_2 \ell_6 \ell_5 \ell_0 \ell_3 \oplus K$)
                $\oplus$SboxRight($\tilde{\ell}_0 \tilde{\ell}_2 \tilde{\ell}_6 \tilde{\ell}_5 \tilde{\ell}_0 \tilde{\ell}_3 \oplus K$)) then
                increment count[K]
            end if
        next K
    end if
next i

These key bits can be guessed separately from the others.

The remaining keys bits can be guessed by exhaustive search with one cipher text.

Thus an overall complexity of about 2^{11} which is better than the exhaustive search over the entire keyspace.

Swept under the rug

What is a good probability?

How many plaintextpairs do we need?

Are there assumptions that we've taken for granted?

Thank you