Computer Security and Networks

Eike Ritter and David Oswald

Today's Lecture

- Introduction to the Module
- Ciphers
  - Frequency analysis
  - One Time Pads
  - AES

What is Computer Security?

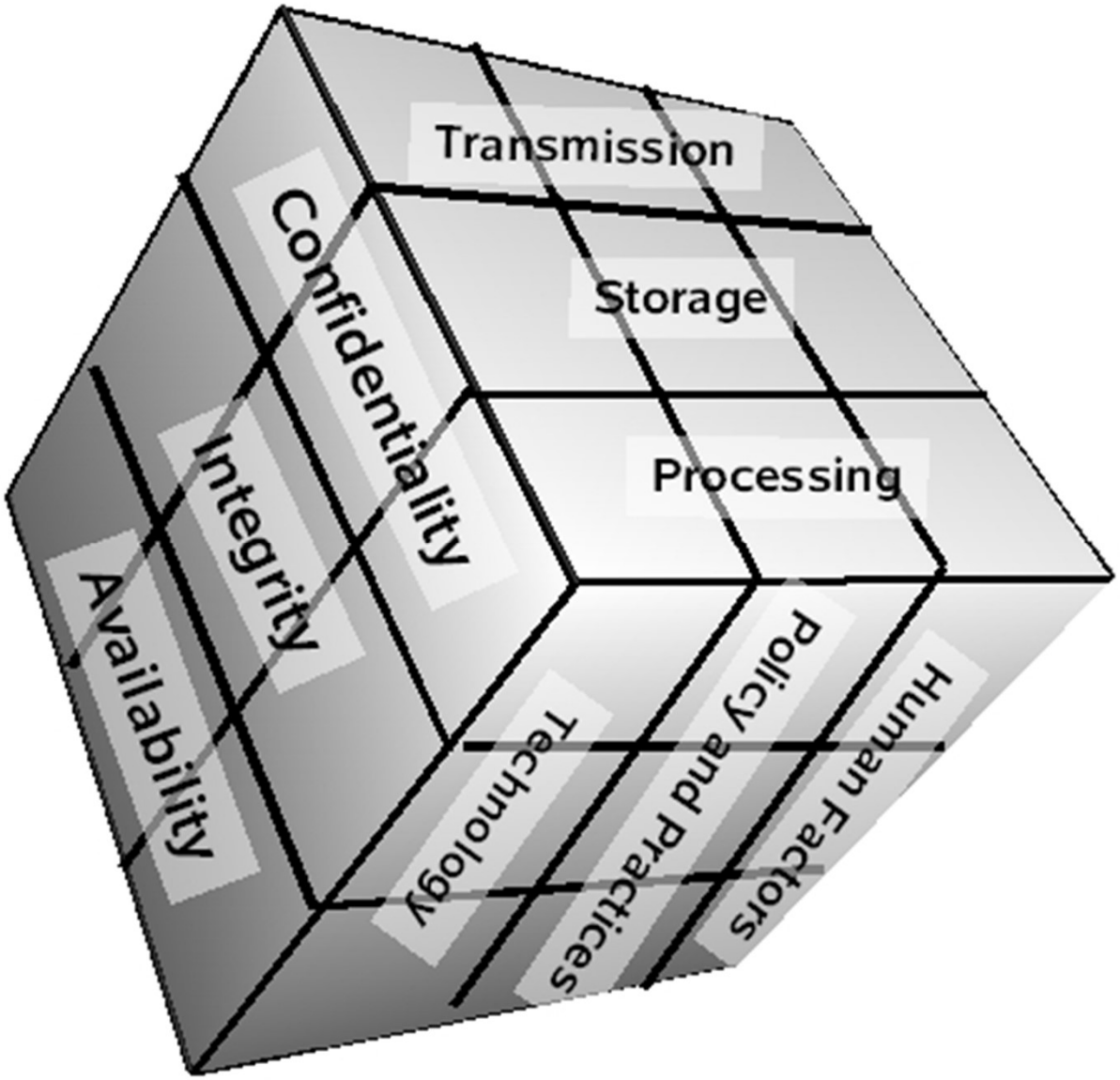
- Correctness and efficiency

What is Computer Security?

- Correctness and efficiency against an attacker.
- Decide what your assets are, estimate the impact of attacks, likelihood, risks, mitigations …
- Analyse systems, spot vulnerabilities, build protection.

What Does Computer Security Protect?

- **Confidentiality**: attacker can't read your data
- **Integrity**: The data I receive is genuine.
- **Availability**: I can get my data when I need it.



McCumber Cube

A framework for thinking about computer security

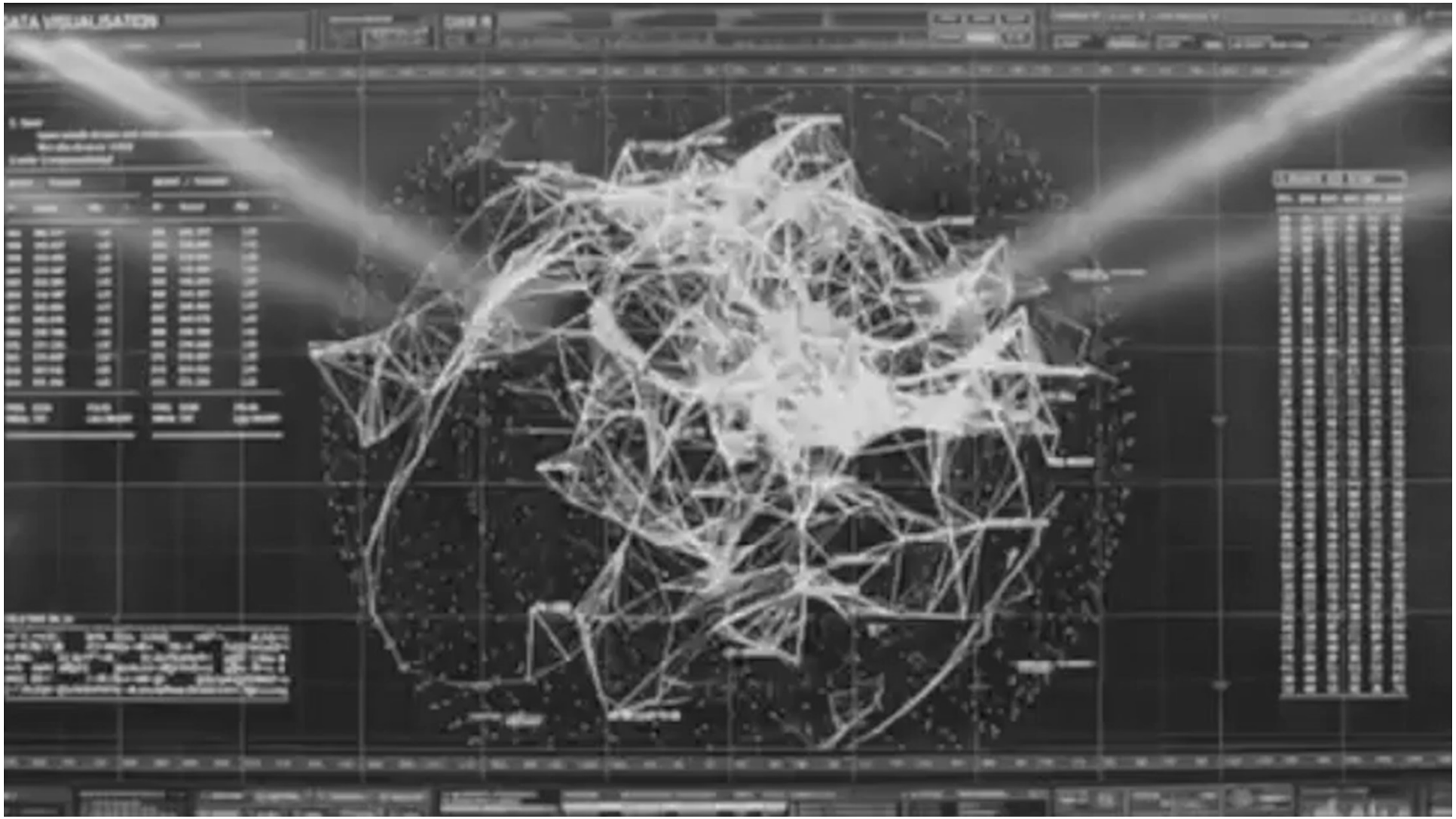
source:wikipedia

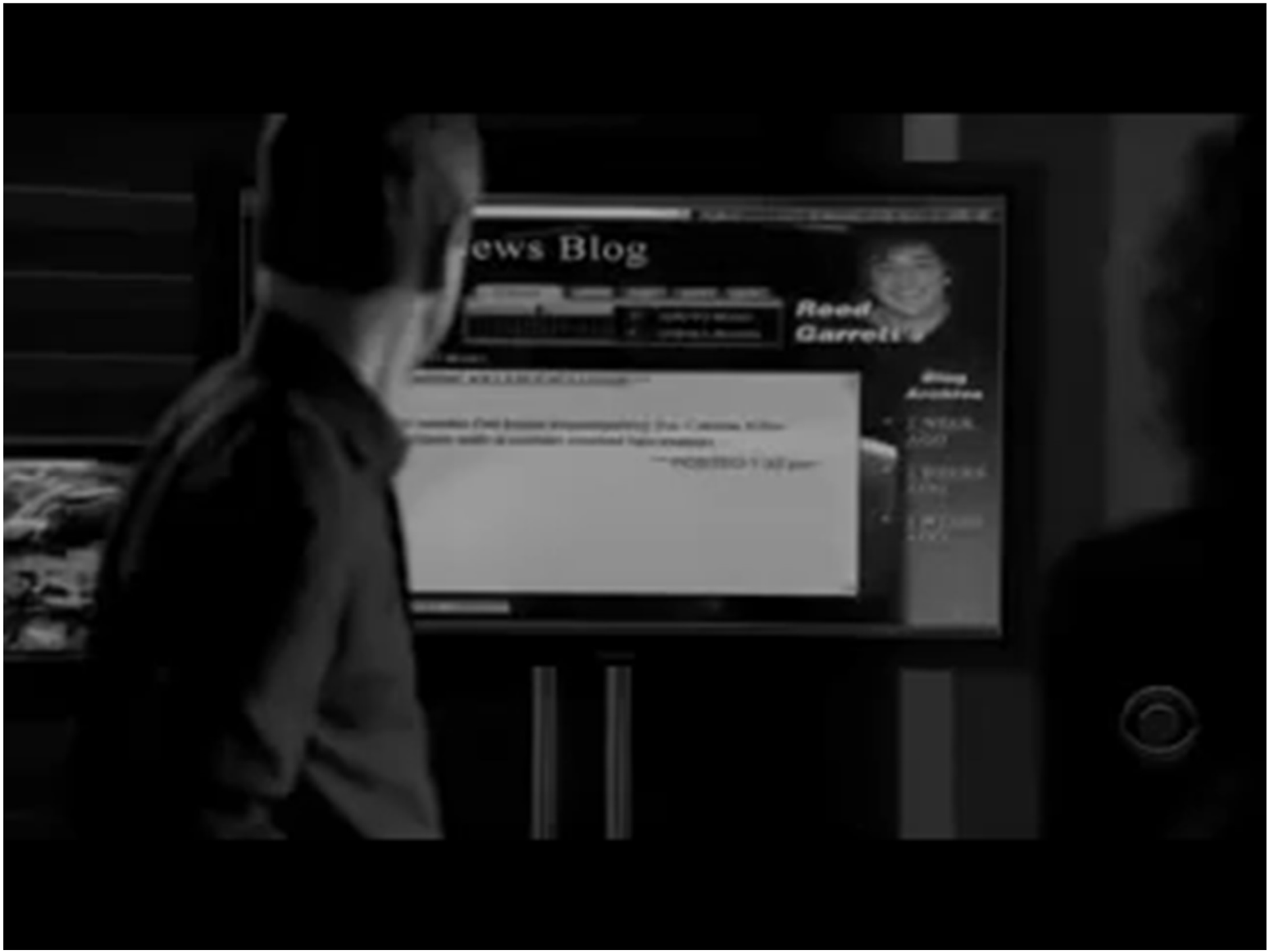
A Threat/Attacker Model

- What are we trying to keep our assets safe from?
- Before building a security system you must state your assumption about what the attacker might try.
- This is known as a threat model or an attacker model.

Attackers

- Lone Hackers, script kiddies.
  - Probably run known attacks using scripts.
- Professional Criminal gangs:
  - Take control of 100,000's of computers via bugs in web-browsers
  - Spam, phishing attacks.
  - DoS attacks
- Governments:
  - Unbelievable computing power
  - Wiretaps
  - Lawyers
- ISPs, Service providers
  - Don't break laws.
  - Do "spy" on you.
  - May sell/loose your data
- Insiders.




ews Blog
Reed
Garrett's


usa

Module Outline

- Cryptography
- Access Control
- Introduction into Networking
- Security protocols
- Web Systems and Attacks
- Other Common Attacks and Defences

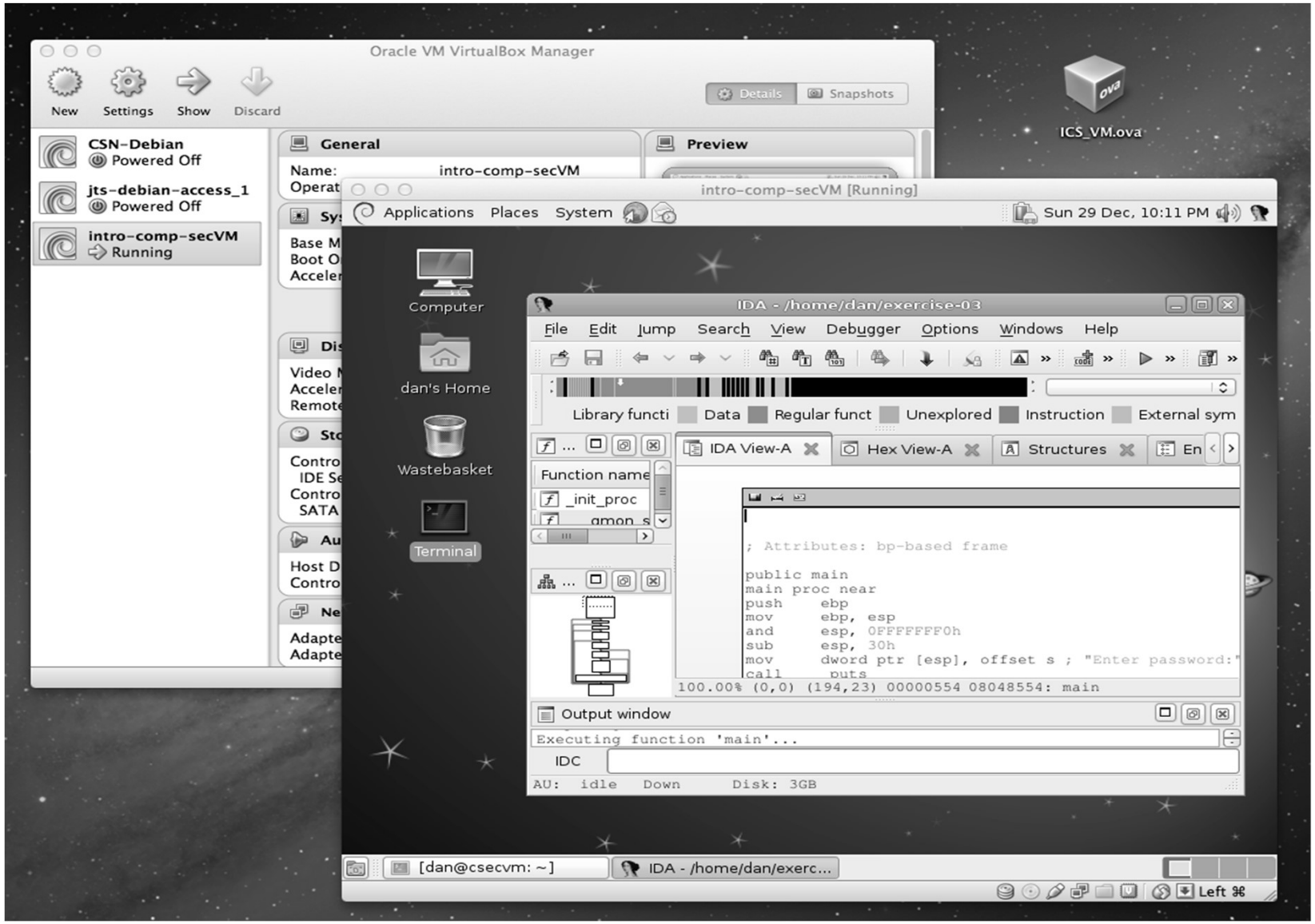
Canvas Page

- Lecture slides.
- Exercises.
- Further reading.

Live Demos

- These lectures will include lots of live demos.
- All live demos are risky, some will go wrong, e.g.,
  - Dropped network connections
  - Crashed program.
- If you want to be shown how to do a demo yourself, see me or a tutor during a lab session.

VM based exercises



Tokens/Flags

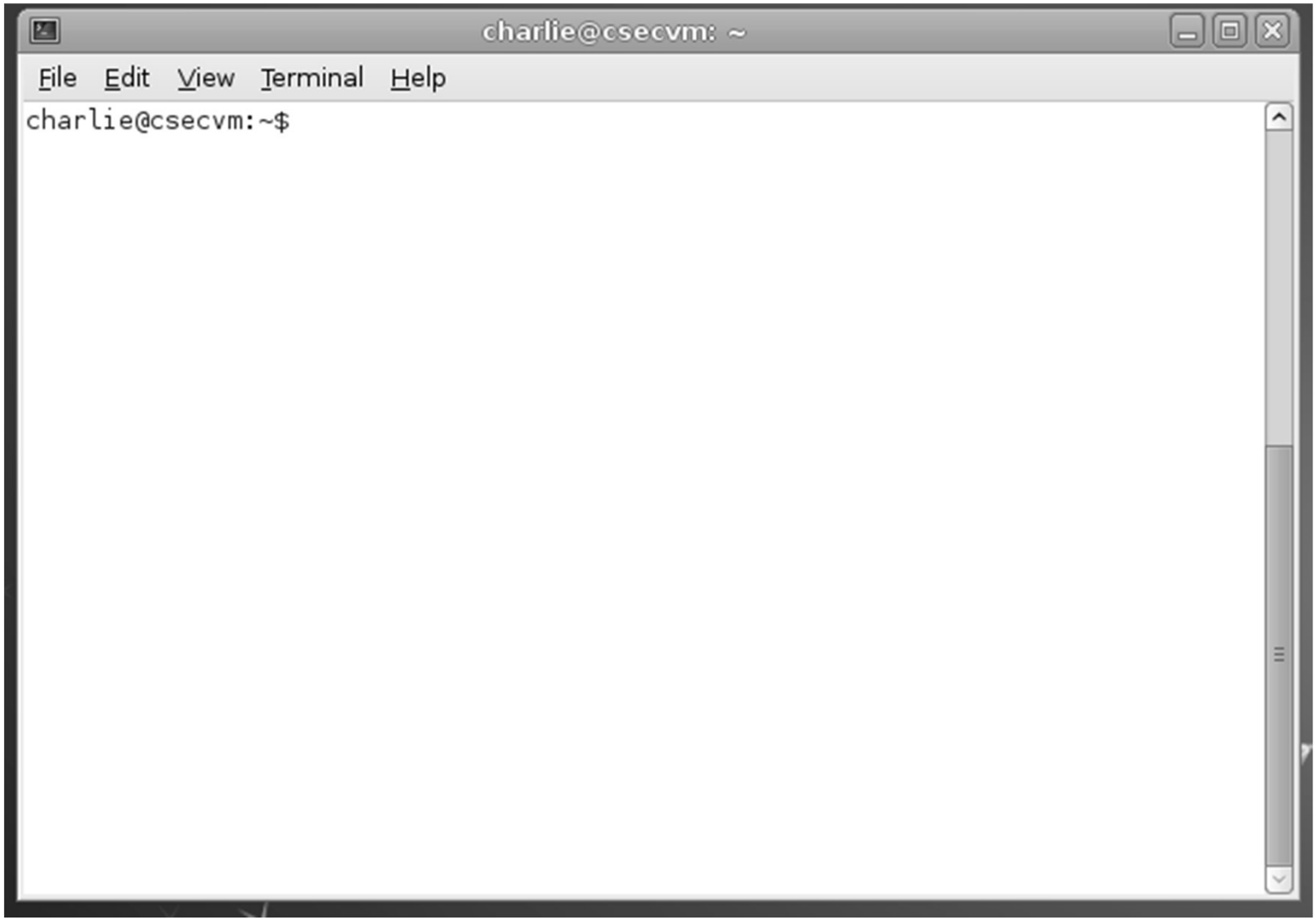
- When you complete an exercise on the VM you will usually find a token (or flag).
- You submit this to a website, to show you have solved the exercise.
- Tokens are unique to your VM. ***You must not share VMs (or tokens).***

DO NOT TRY OUT ANYTHING ON COMPUTERS YOU DON'T OWN

- It is illegal to access computers without the owner's permission.
- Most access is logged, and it's easy to get caught.
- Trying something "just for fun" could get you kicked out of the University.

Command Line

Command Line



Should you take this module?

- This module is about how systems fail.
- So, you need a good understanding of how systems work.
  - Java, Jar files,
  - Websites: HTML, JavaScript, SQL, HTTP,..
  - Good mathematics (modulo arithmetic, power laws)

Plagiarism

- Do not copy answers. Do not copy tokens. Do not let someone copy from you.
- You do not have to answer very questions. No answer is fine.
- ***Any*** Plagiarism will results in either your exercise, or entire coursework, mark zeroed.

Your answer:
Firstly I signed up on the website and logged in. I analysed the cookies of the website and one of the cookies looked unusual. I copied it and decrypted the md5 hash and it gave me a value of 0. Then I encrypted 1 and put it instead of the zero and put the cookie back in Firefox plugin. As soon as I went back to the website, it turned into a black market

Your answer:

- I made an account in the website
- Then I logged in into the website using that login information.
- I inspected the cookies of the site, and found a cookie that looked unusual as its name looked hashed. It had a value that looked like an md5 hash.
- I decrypted it and found it is equal to 0, so I assumed it meant to be a boolean variable that indictes if the black market should be activated or disactivated.
- Therefore, I encrypted 1 using md5, and used a firefox plugin to set the cookies to the encrypted value of 1.
- After refreshing the page I got access into the black market.

[redacted] [redacted] 16/03/2015 23:49

get your [redacted] tokens out of here [redacted]

[redacted] [redacted] 17/03/2015 00:05

```
<?php
$homepage = file_get_contents('http://www.example.com/');
echo $homepage;
?>
```

[redacted] [redacted] 17/03/2015 00:28

mysql -h 127.0.0.1 -u <username> -p

[redacted] [redacted] 17/03/2015 00:33

28670cbc760f0f73112c067c79004a19

[redacted] [redacted] 17/03/2015 00:33

d66c7e83862867fde8d8bc9923e02cc5

[redacted] [redacted] 17/03/2015 01:51

youz good geezer?

[redacted] [redacted] 17/03/2015 01:51

Yeah mate

Today's Lecture

- Introduction to the Module
- Ciphers
  - Frequency analysis
  - One Time Pads
  - AES

Codes vs. Ciphers

- A code is any way to represent data. E.g.
  - Morse Code, ASCII, Hex, Base64, Binary,…
- A cipher is a code that it designed to be hard to read.
  - Almost always uses a key.

Codes vs Cipher

What is “27” in binary?

a) 0010 1011
b) 0001 1011
c) 00110010 00110111
d) 00100111
e) All of the above.

Codes vs Cipher

What is “27” in binary?

a) 0010 0111
b) 0001 1011
c) 00110010 00110111
d) 00100111
e) All of the above ✔

Codes vs Cipher

What is “27” in binary?

a) 0010 0111
b) 0001 1011
c) 00110010 00110111
d) 00100111
e) All of the above ✔

27 as decimal
27 as hex
27 as ASCII
27 as Base64

Hex

0 = 0000
1 = 0001
2 = 0010
3 = 0011
4 = 0100
5 = 0101
6 = 0110
7 = 0111

8 = 1000
9 = 1001
A = 1010
B = 1011
C = 1100
D = 1101
E = 1110
F = 1111

- Characters 0 to F encode 4 bits.
- Easiest way to write down binary as text.
- 27 = 0010 0111

Hex	Dec	Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x00	0	NULL	null	0x20	32	Space	0x40	64	@	0x60	96	`
0x01	1	SOH	Start of heading	0x21	33	!	0x41	65	A	0x61	97	a
0x02	2	STX	Start of text	0x22	34	"	0x42	66	B	0x62	98	b
0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	c
0x04	4	EOT	End of transmission	0x24	36	$	0x44	68	D	0x64	100	d
0x05	5	ENQ	Enquiry	0x25	37	%	0x45	69	E	0x65	101	e
0x06	6	ACK	Acknowledge	0x26	38	&	0x46	70	F	0x66	102	f
0x07	7	BELL	Bell	0x27	39	'	0x47	71	G	0x67	103	g
0x08	8	BS	Backspace	0x28	40	(	0x48	72	H	0x68	104	h
0x09	9	TAB	Horizontal tab	0x29	41	)	0x49	73	I	0x69	105	i
0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0C	12	FF	Form Feed	0x2C	44	,	0x4C	76	L	0x6C	108	l
0x0D	13	CR	Carriage return	0x2D	45	-	0x4D	77	M	0x6D	109	m
0x0E	14	SO	Shift out	0x2E	46	.	0x4E	78	N	0x6E	110	n
0x0F	15	SI	Shift in	0x2F	47	/	0x4F	79	O	0x6F	111	o
0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0x72	114	r
0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	s
0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	w
0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	y
0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x1B	27	FSC	Escape	0x3B	59	;	0x5B	91	[	0x7B	123	{
0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\	0x7C	124	|
0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93	]	0x7D	125	}
0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95	_	0x7F	127	DEL

Base64

Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P

Binary	ASCII
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z
011010	a
011011	b
011100	c
011101	d
011110	e
011111	f

Binary	ASCII
100000	g
100001	h
100010	i
100011	j
100100	k
100101	l
100110	m
100111	n
101000	o
101001	p
101010	q
101011	r
101100	s
101101	t
101110	u
101111	v

Binary	ASCII
110000	w
110001	x
110010	y
110011	z
110100	0
110101	1
110110	2
110111	3
111000	4
111001	5
111010	6
111011	7
111100	8
111101	9
111110	+
111111	/

Shortest way to write binary as printable characters.

Common for keys & crypto

This module will use hex

Code demo

Caesar Cipher

- One of the first codes was used by Julius Caesar.

- The Caesar Cipher replaces each letter of the alphabet with one three to the right, i.e.
  - a becomes d,
  - b becomes e,
  - ....
  - z becomes c.

Using a Key

- These ciphers are easy to break because as soon as you know the scheme you can decrypt the message.

Kerckhoffs's principle: A cipher should be secure even if the attacker knows everything about it apart from the key.

Using a Key

- For instance, we can use the Caesar cipher rotating “n” rotations.

VIGENERE TABEL

PLAIN TEXT

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
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

source:wikipedia

VIGENERE TABEL

PLAIN TEXT

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
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

source:wikipedia

VIGENERE TABEL

PLAIN TEXT

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
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

ROT13

source:wikipedia

Using a Key

- For instance, we can use the Caesar cipher rotating “n” rotations.

- But only 26 possible keys so you can just try them all (breaking the cipher is 26 times harder without the key).

Using a Key

- For instance, we can use the Caesar cipher rotating “n” rotations.
- But only 26 possible keys so you can just try them all (breaking the cipher is 26 times harder without the key).
- A better scheme replaces each letter with another letter. Here there are $26! \approx 4 \times 10^{26}$ possible keys.

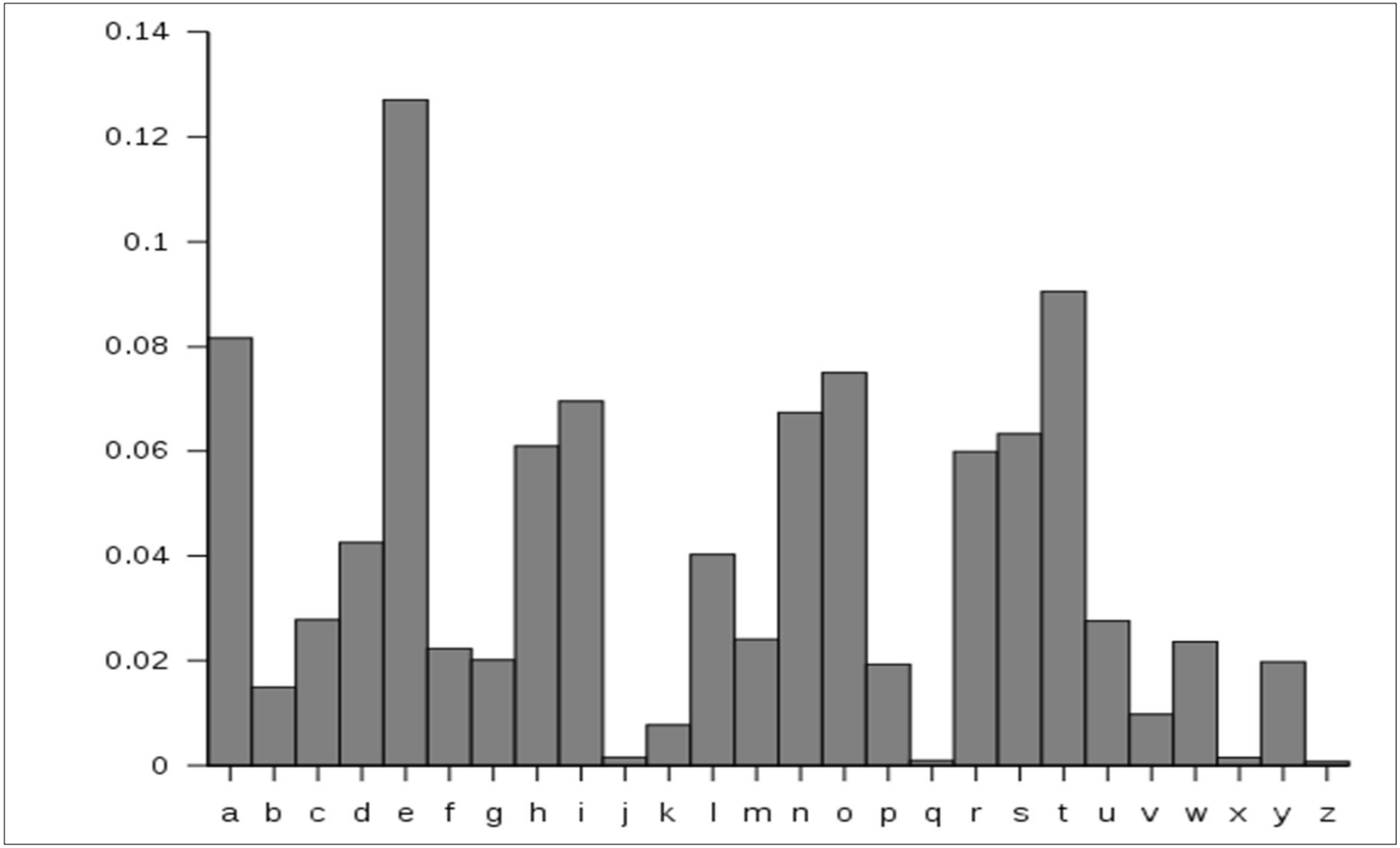
Frequency Analysis

- While hard to break by brute force, replacing each letter with another is easy to break using *frequency analysis*.

- Frequency analysis counts the number of times
  - each symbol occurs
  - each pair of symbols
  - etc.

  and tries to draw conclusions from this.

Frequency Analysis



picture for wikipedia GNU

One Time Pads

- Perfect encryption
- Needs a key as long as the message.

Message:
Key:
Cipher text:

One Time Pads

- Perfect encryption
- Needs a key as long as the message.

Message: HELLOALICE
Key:
Cipher text:

One Time Pads

- Perfect encryption
- Needs a key as long as the message.

Message: HELLOALICE
Key: SGFKPQYEIJ
Cipher text:

VIGENERE TABEL

PLAIN TEXT

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
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

source:wikipedia

One Time Pads

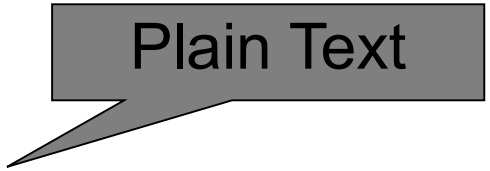
- Perfect encryption
- Needs a key as long as the message.

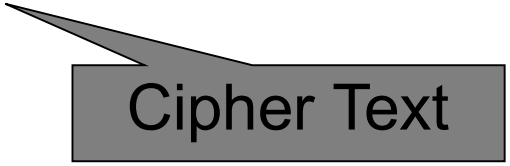
Message: HELLOALICE
Key: SGFKPQYEIJ
Cipher text: ALRWERKNLO

One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Message: HELLOALICE
Key: SGFKPQYEIJ
Cipher text: ALRWERKNLO





One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text ALRWERKNLO

One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text ALRWERKNLO
Key: SGFKPQYEIJ

One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text ALRWERKNLO
Key: SGFKPQYEIJ
Message: HELLOALICE

One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text ALRWERKNLO

One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text ALRWERKNLO
Key: TWCSCTFLWM

One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text ALRWERKNLO
Key: TWCSCTFLWM
Message: GOODBYEBOB

Xor ⊕

0 xor 0 = 0
1 xor 0 = 1
0 xor 1 = 1
1 xor 1 = 0

(M ⊕ k) ⊕ k = M

ascii

Hello Alice → 01011001 01100101 01110011

Key
11001011 01001101 11110001 →

10010010 00101000 10000010

Xor ⊕

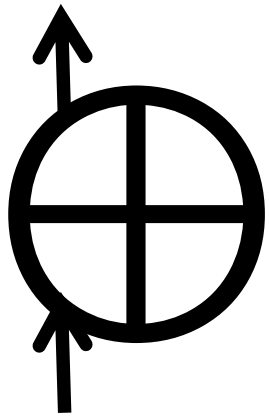
0 xor 0 = 0
1 xor 0 = 1
0 xor 1 = 1
1 xor 1 = 0

$(M \oplus k) \oplus k = M$

ascii

Hello Alice ← 01011001 01100101 01110011

Key
11001011 01001101 11110001 →



10010010 00101000 10000010

One Time Pads

- Problem?

One Time Pads

- Problem
  - The key needs to be as long as the message.
- Russia during and after W.W.2
  - Reused the key material
  - Broken by the Venona project.

Block Ciphers

- Modern ciphers work on blocks of plain text, not just a single symbol.
- They are made up of a series of ***permutations*** and ***substitutions*** repeated on each block.
- The key controls the exact nature of the permutations and substitutions***.***

Advanced Encryption Standard (AES)

- AES is a state-of-the-art block cipher.
- It works on blocks of 128-bits.
- It generates 10 round keys from a single 128-bit key.
- In uses one permutation: ShiftRows and three substitutions SubBytes, MixColumns, AddRoundKey.

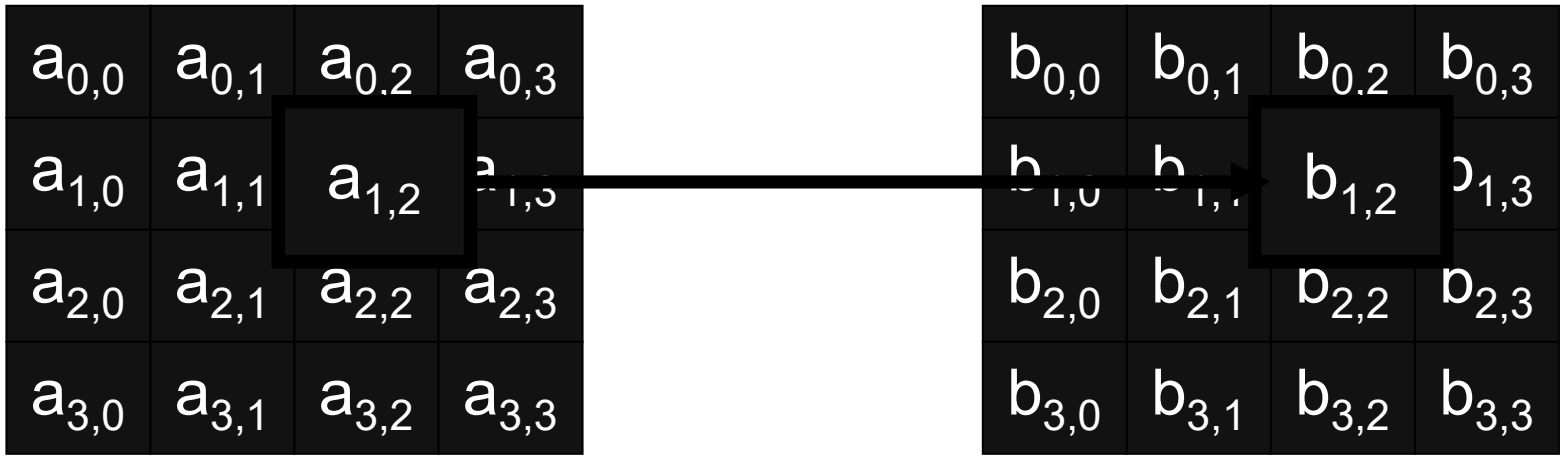
Modulo Arithmetic

- Arithmetic modulo “n” means that you count up to “n-1” then loop back to 0
- i.e., 0,1,2,...,n-1,0,1,2,...,n-1,0,1,2,...

- a mod b = r for largest whole number k such that a = b.k + r

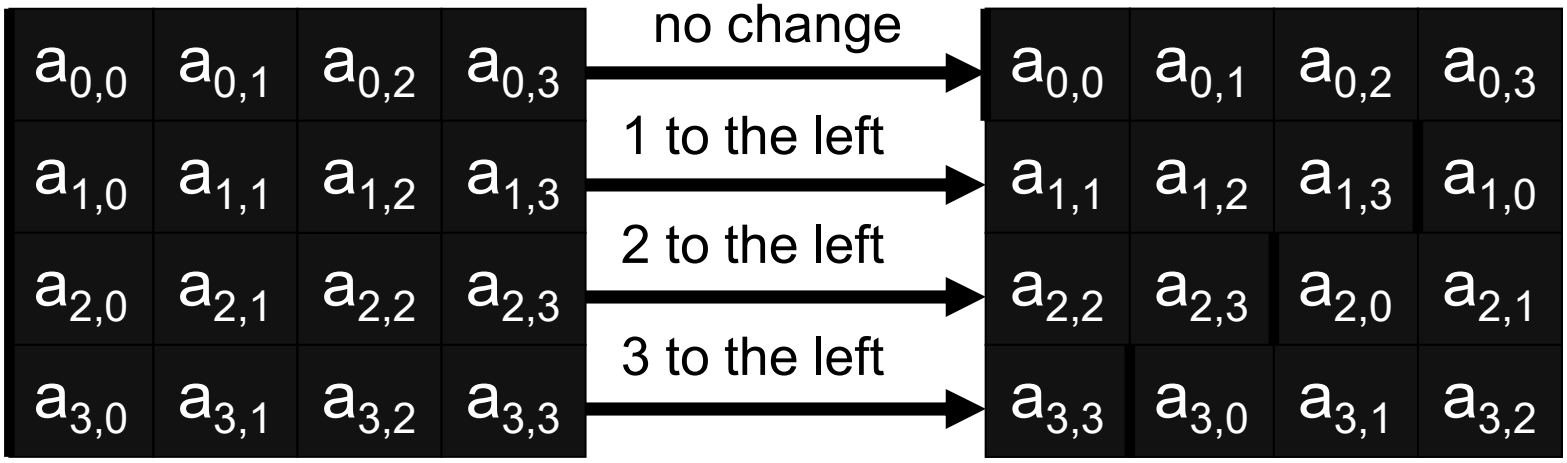
- e.g. 9 mod 4 = 1 because 9 = 2.4 +1

SubBytes: S-box



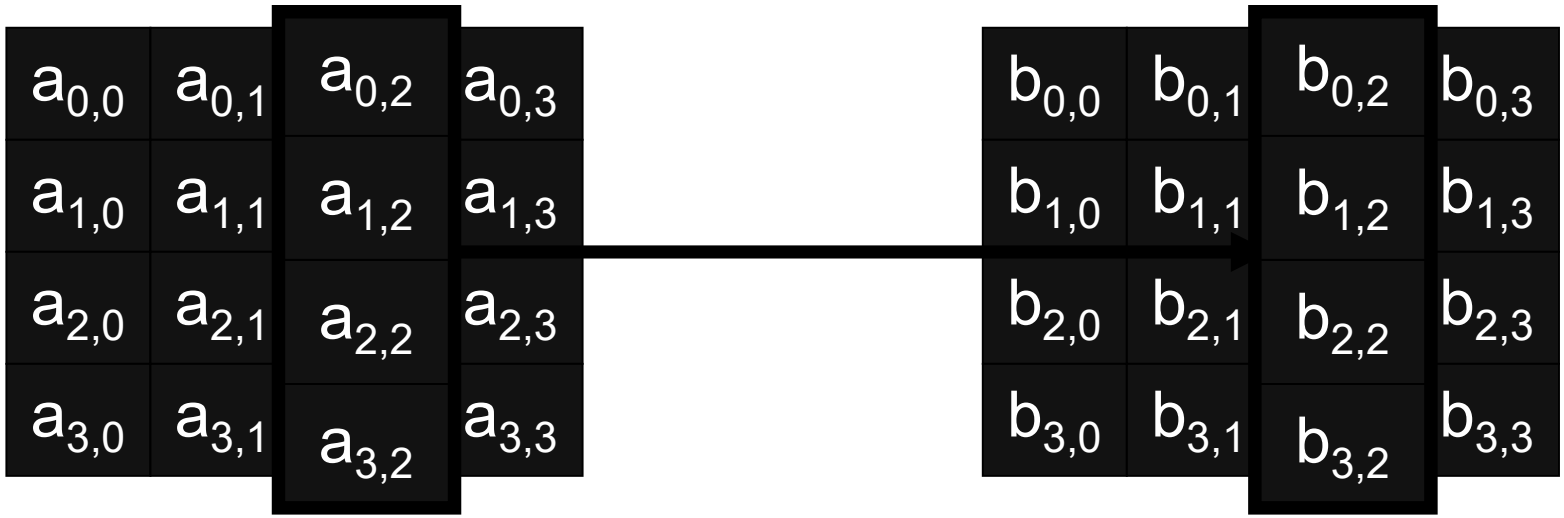
- The "SubByte" is a fixed substitution based on matrix multiplication, one byte at a type.

ShiftRows



- "ShiftRows" moves the
  - 2nd row one byte to the left,
  - the 3rd row two bytes
  - and the 4th row 3 bytes.

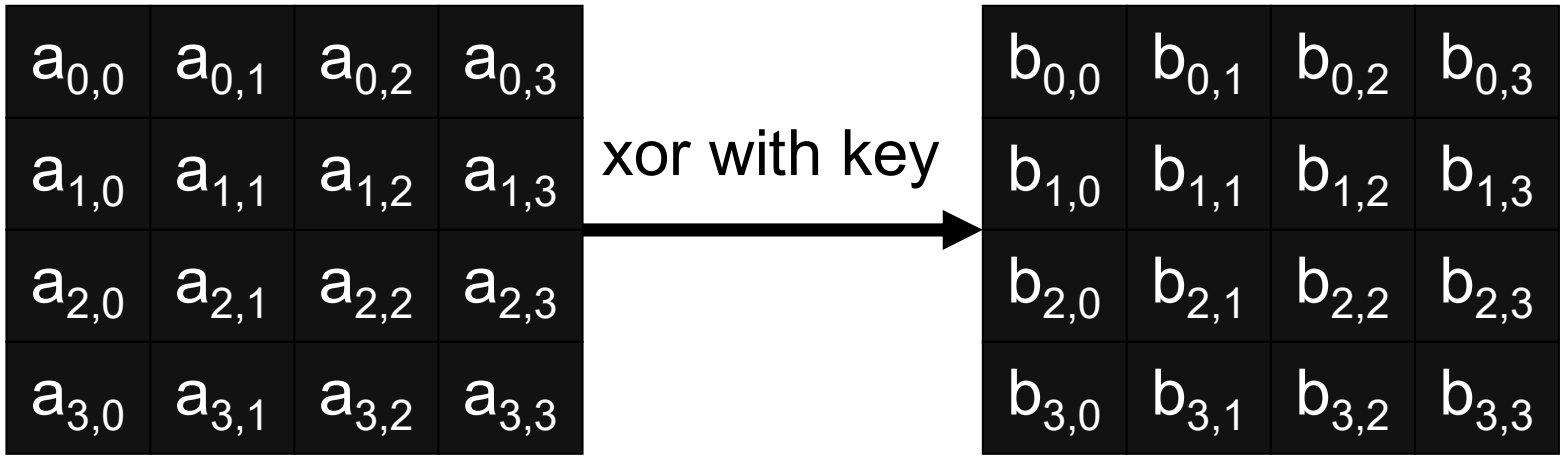
MixColumn



- "MixColumn" is a substitution of each column such that:

$$(a_0.x^3 + a_1.x^2 + a_2.x + a_3) \times (3.x^3 + x^2 + x + 2) \bmod (x^4+1) = (b_0.x^3 + b_1.x^2 + b_2.x + b_3)$$

AddRoundKey



- "AddRoundKey" xor's the block with the 128-bit round key (which was generated from the main key).
  - $b_{i,j} = a_{i,j}$ xor $k_{i,j}$

AES

- AES encrypts data by first generating the round keys from the main key
- Then 9 rounds of:
  1. SubBytes
  2. ShiftRows
  3. MixColumns
  4. AddRoundKey
- Finally:
  1. SubBytes
  2. ShiftRows
  3. AddRoundKey

AES demo

- Gen Key
- Enc

Next Steps:

- Modern Block Ciphers
  - AES, DES and 3-DES
- How to encrypt more than one block
- Block cipher modes
  - ECB, CBC, CTR