Learning Cryptography through handcyphers

or the encryption 101

If you

understand the basics of
cryptography

you're more able to understand
the tools and thus
apply the technology better

It's not too complex!

In this hour

- Who's bullshitting today?
- Why cryptography?
- Working on handcyphers?
- Now what?

In this hour

- **Who's bullshitting today?**
- Why cryptography?
- Working on handcyphers?
- Now what?

Who's bullshitting today?

- Brenno de Winter, 34, single, male, open source minded, freedom loving, technology savvy, stubborn, community playing, overactive, news junk.
- Started programming at age of 6, explored the security options in the world

Who's Bullshitting today?

- Today I'm freelancejournalist

for several publications, so I:

  - Write about technology;
  - Teach it;
  - Talk about it;
  - Consult it;
  - Participate in the community.

NEDLINUX.NL

In this hour

- Who's bullshitting today?
- Why cryptography?
- Working on handcyphers?
- Now what?

Why cryptography?

Because it is a security tool helping us

keep secrets secret

and help us perform

authentication

Cryptography is

a great privacy tool

Privacy? I've got nothing to hide

- Well you do! Wanna debate? After the session
- It is a civil liberty and a human right
- Needed for:
  - fundamental basis for maintaining democracy;
  - thus protection from totalitarian-regimes;
  - needed to maintain freedom of speech;
  - a personal live;
  - protection against crimes;
  - protection against data theft;

The question is really

Who do we award with privacy
and who should be transparent?

Are you afraid of your government?

- Yes! They can't deal with information:
  - Dutch lawful interception centers are not protected well enough (study);
  - DA's place their computer with sensitive data and their kiddy porn on the street as garbage;
  - Clueless agents share sentive files through Kazaa;
  - Laptops with data (unencrypted) were stolen from a police station
  - The secret service leaves state secrets in rental cars and laptops in train;
  - There is little democratic control on secret service;

So encryption?

Yeah to decrease the change
of abuse by third parties

In this hour

- Who's bullshitting today?
- Why cryptography?
- **Working on handcyphers?**
- Now what?

Working on handcyphers?

Well good to understand
how algorithms grew to what they are

Handcyphers: Basically pen and paper algorithms

Ceasar Rotation (ROT)

- The alphabet shifts x-positions
- ROT-13

ABCDEFGHIJKLMNOPQRSTUVWXYZ ->

NOPQRSTUVWXYZABCDEFGHIJKLM

So: CHAOS COMPUTER CAMP becomes
PUNAE PAYBGFRD PNYB

Downside

- Easy to crack, only 26 options
- ROT-13 is the most popular so a good starting point
- It was still used “professionally” in 2001

Mono Alphabetic substition

Every letter is replaced by another character

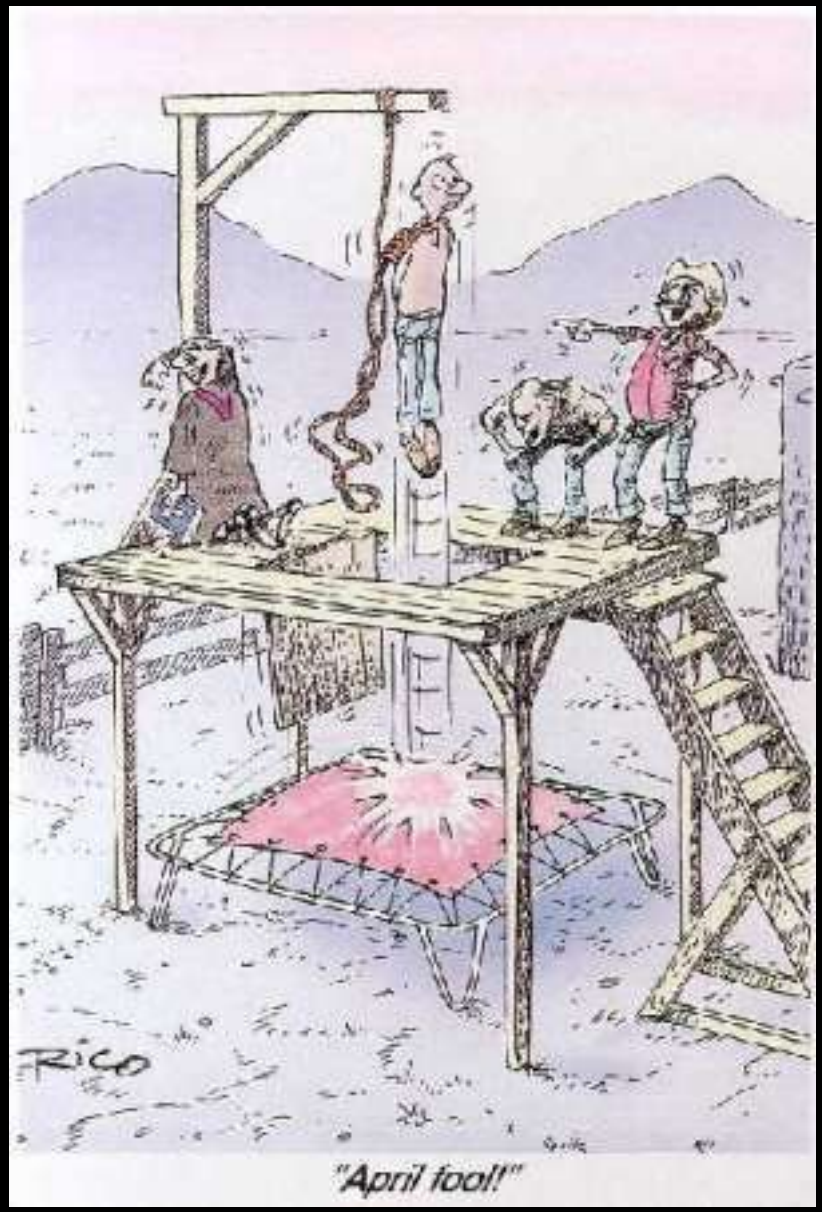
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	D	K	I	C	Y	R	S	J	L	X	Z	N	P	M	G	R	T	U	V	O	W	F	A	H	E

“Legal” becomes “Zcrbz”

No we're “totally secure”, since we have 26*25*...*1 possibilities

Also limited in protection

- Did you ever play Hangman?



So this can be cracked too?

- The code was safe until the 9th century when statistical data on character usage was found
- No alternative available until 1553

Character	Times per 1,000 characters
E	159
N	86
A	63
T	56
R	54
D	51
O	48
I	47
S	35
L	31
G	28

Vigenère

- Use of encryption through a shared key
- Using poly alphabetic substitution
- Giovanni Batista Belaso inventor, Blaise de Vigenère made the world aware

	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

Using the table

- Encryption goes like this

```
LEGALILLEGALSCHEISSEGAL
SECRETSECRETSECRETSECRE
DIIRPBDPGXEEKGJVMLKIIRP
```

- Remarks:
  - Of course ought to be without spaces
  - Exchanging passphrase is a pain
  - How many shared secrets do you need?

Cracking

- Shared secret is the key -> longer passphrases make the algorithm stronger
- Phrase repeats itself, so it can be cracked

Enhancing with autokey

- The solution is using infinite keys
- Using the message as a key
- Keyword: SECURITY
- Message: THIS IS AN IMPORTANT MESSAGE
- Rolling keyword: SECURITYTHISISANIMPORTANTMESSAGE

Homophone Substitution

- Alternative to polyform substition
- Attachting multiple numbers to a letter
- A 11 28 48 62 64
- B 10 37
- C 20 47 61
- D 00 38 59
- E04 25 29 49 60 63 73
- etc.

Substitution isn't enough

- Characters are still replaced
- Experience will lead to cracking
- Solution: shuffling of characters

Bifid-table

- We build a 5 by 5 table based on a passphrase
- Passphrase: hackersconference
- Message: I understand cryptography

The table

	1	2	3	4	5
1	H	A	C	K	E
2	R	S	O	N	F
3	B	D	G	I	J
4	L	M	P	Q	T
5	U	V	W	XY	Z

The first coding

- Message: IUNDERSTANDCRYPTOGRAPHY
- Horizontal: 41425125242314353312314
- Vertical: 352312241231254232 1415
- Now encrypt with the numbers per line
- so 41 42 51 .... 35 23 12 24
- Encrypted: KNEVMDLWGRCXDRMRCVQDAKU

In this hour

- Who's bullshitting today?
- Why cryptography?
- Working on handcyphers?
- Now what?

Now what?

- Use what you know, play with it
- Keep learning and learn more cyphers
- Learn about PKI and PGP
- Code open source apps
- Work on user-friendly encryption technologies
- Use it in: e-mail, webservers, instant messaging, etc.
- Don't stop defending civil liberties

Share knowledge!

Subscribe to my monthly newsletter
Dutchies listen to my podcast (http://ictroddels.nl)
it's free

http://dewinter.com - brenno@dewinter.com
(C222 6DD2 8BB9 9DD9 0EFD
73DF 306B 21C2
A094 F1D9)