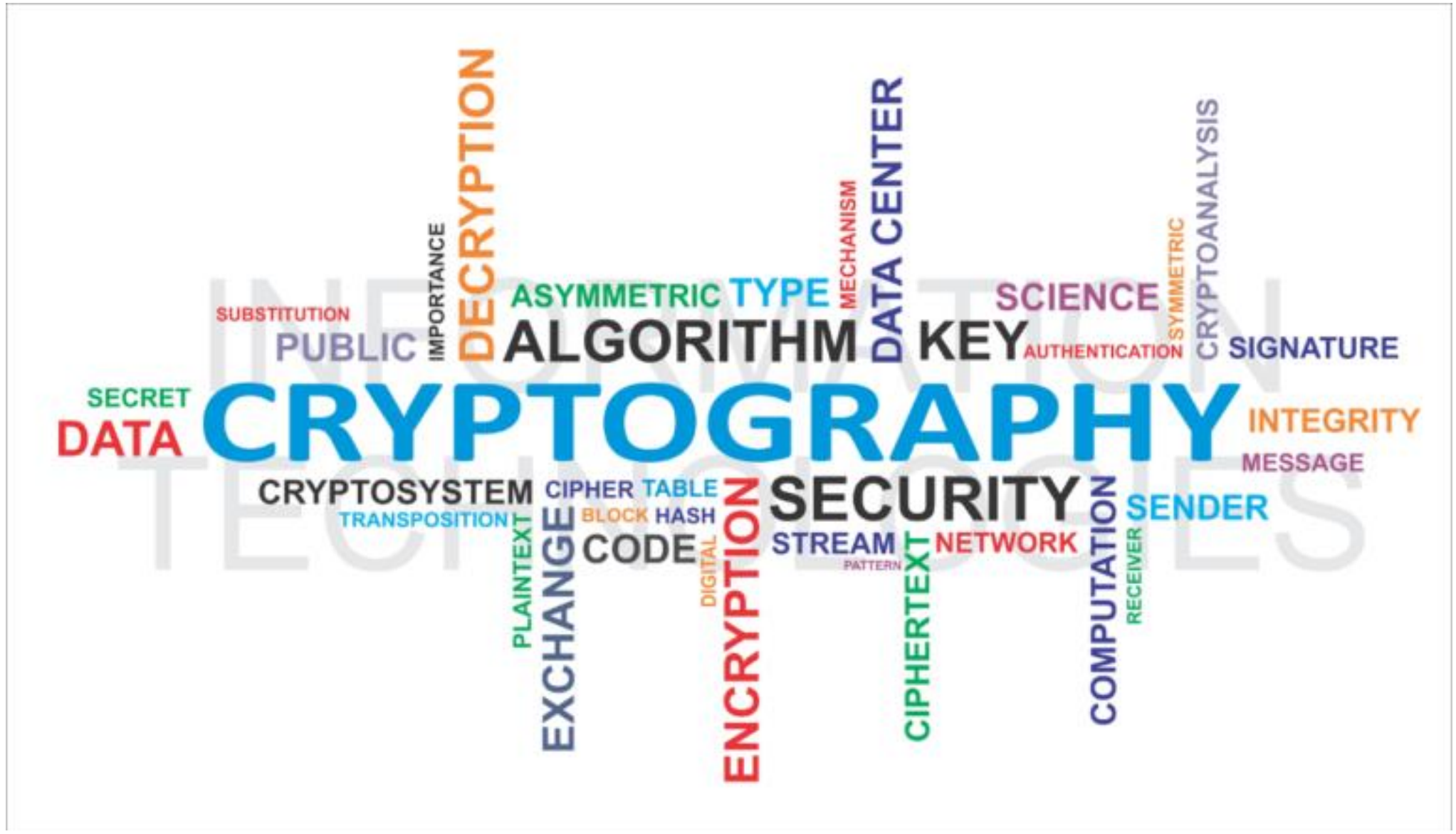
NEMATYC 2018

Massachusetts Maritime Academy

Exploring Cryptography Using CrypTool

Valeria D'Orazio – Massachusetts Maritime Academy


CRYPTOGRAPHY
DATA
SECRET
ALGORITHM
KEY
PUBLIC
SUBSTITUTION
IMPORTANCE
DECRYPTION
ASYMMETRIC
TYPE
MECHANISM
DATA CENTER
SCIENCE
SYMMETRIC
CRYPTOANALYSIS
AUTHENTICATION
SIGNATURE
INTEGRITY
MESSAGE
SECURITY
CRYPTOSYSTEM
CIPHER
TABLE
BLOCK
HASH
TRANSPOSITION
CODE
STREAM
NETWORK
PATTERN
SENDER
RECEIVER
COMPUTATION
CIPHERTEXT
ENCRYPTION
DIGITAL
PLAINTEXT
EXCHANGE

Importance of Cryptography

amazon

MoneyGram®
money transfer

be aware of
your
data

1998 Project start

Originated as an internal business application for information security training for employees of a large German bank .

Developed in cooperation with universities (improvement of education)

Over 50 volunteer developers worldwide contribute to the program.

2003 CrypTool becomes **open source**

www.cryptool.org

www.cryptool.org

CRYPTOOL PORTAL

Cryptography for everybody

E-Learning Software:

CrypTool 1 runs under Windows – 1998

CrypTool 2 runs under Windows – 2011

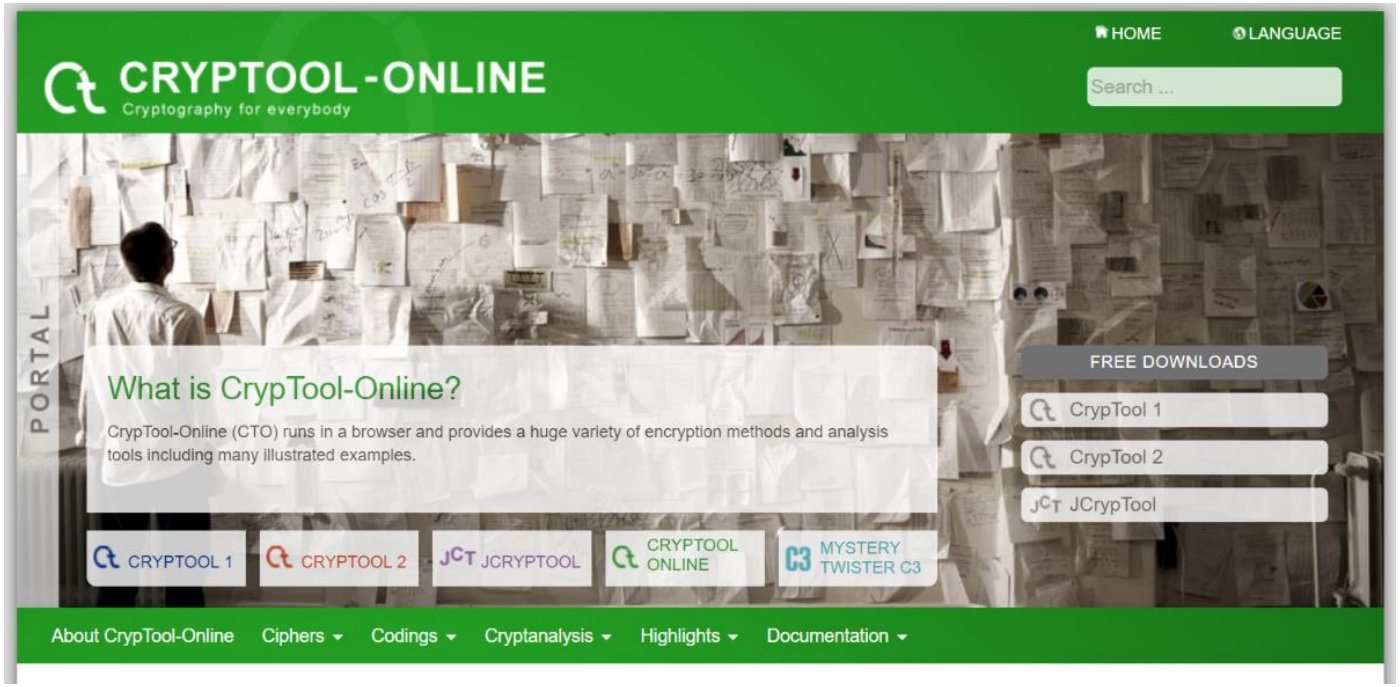
JCrypTool (JCT) runs under Linux, Mac and Windows – 2011

CrypTool-Online - 2009

International crypto cipher challenge "MTC3"
Additional Website available on http://www.mysterytwisterc3.org

CrypTool-Online is the online version of the e-learning program CrypTool.

CrypTool-Online allows to try out different algorithms in a browser / smartphone. Experiment with the introduced methods in an interactive way directly on the website.



CrypTool 1 is available in 6 languages German, English, Spanish, Polish, Serbian and Greek.

CrypTool 1 The current version of CrypTool 1 offers among other things:

Numerous classic and modern cryptographic algorithms (encryption and decryption, key generation, secure passwords, authentication, secure protocols, etc.)

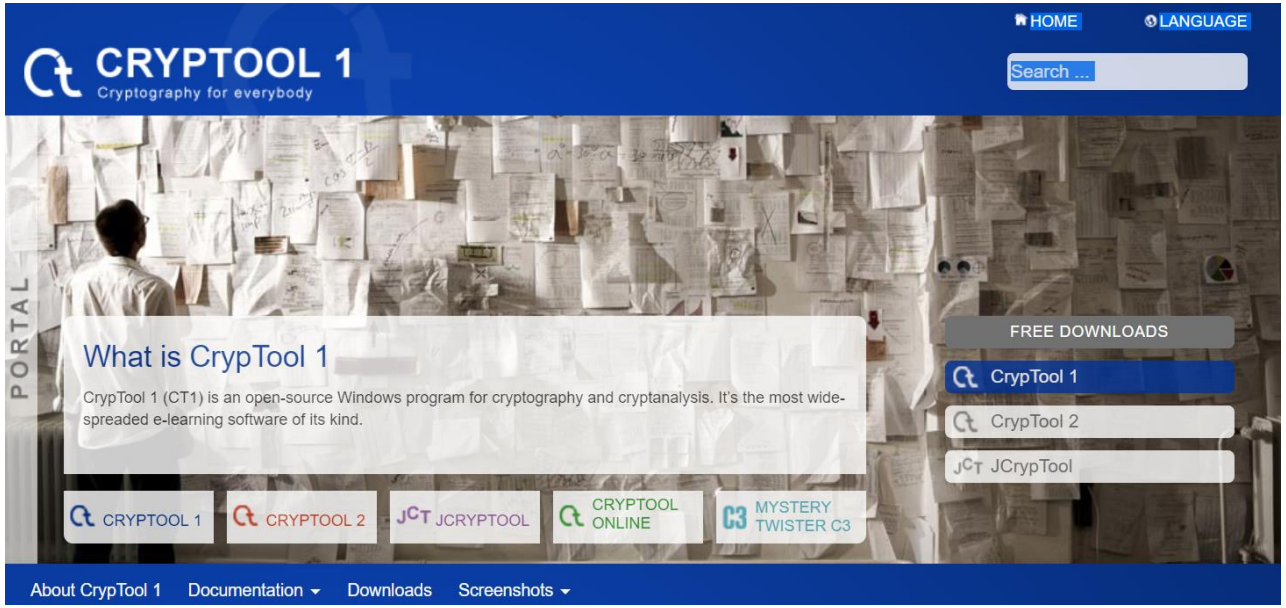
Visualization of several algorithms (Caesar, RSA, Diffie-Hellman, digital signatures, AES, etc.)

Cryptanalysis of several algorithms (Vigenère, RSA, AES, etc.)

Related auxiliary methods (primality tests, factorization, base64 encoding, etc.)

Number theory tutorial

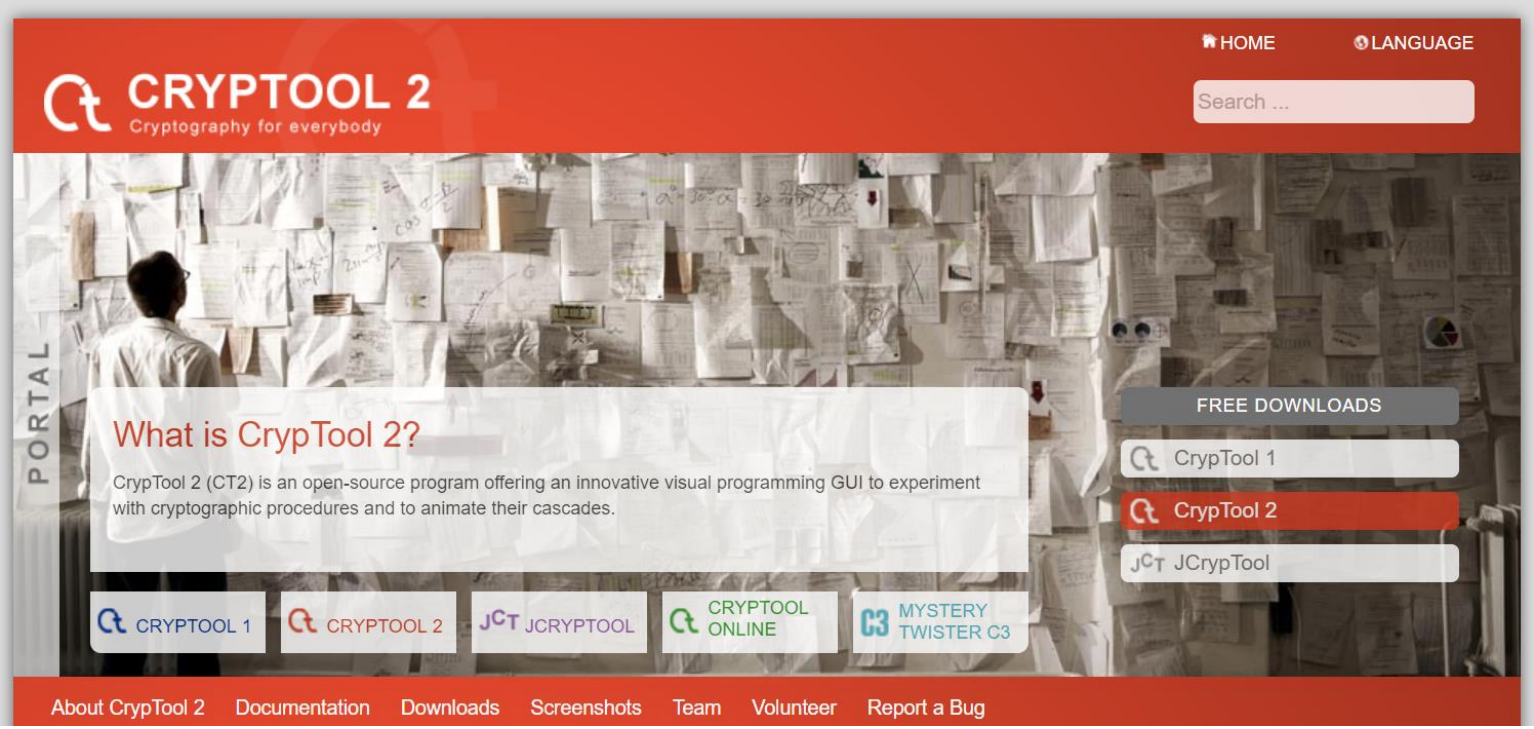
Comprehensive online help



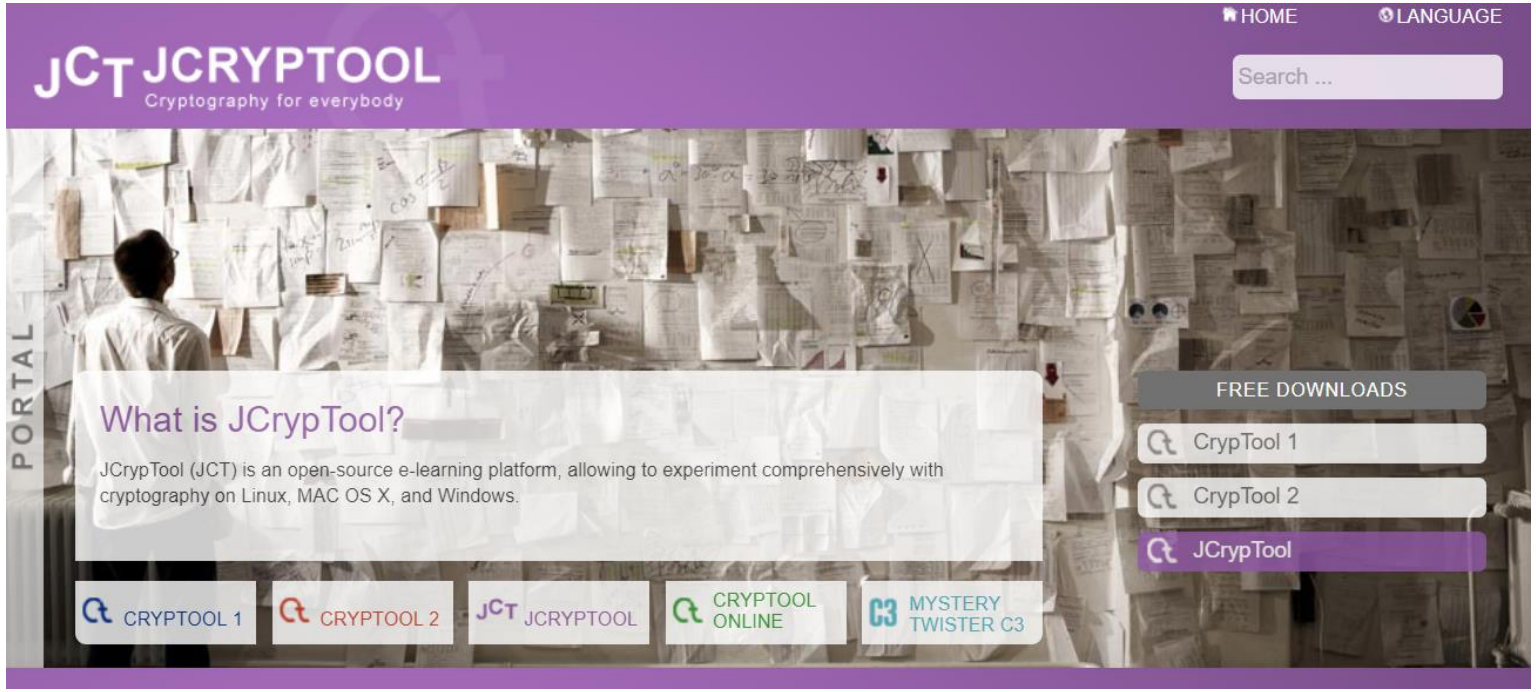
CrypTool 2 is the modern successor of CrypTool 1.

CrypTool 2 provides a graphical user interface for visual programming. So workflows can be visualized and controlled to enable intuitive manipulation and interaction of cryptographic functions.

CrypTool 2 provides a greater variety of cryptanalytical tools to analyze or even break classical and modern ciphers. For instance, it is possible to apply a ciphertext-only attack on an Enigma-encrypted ciphertext.



JCrypTool is an open-source e-learning platform, developed to not only let everybody experiment with cryptography, but to develop and extend the JCrypTool platform in various ways with their own crypto plug-ins.

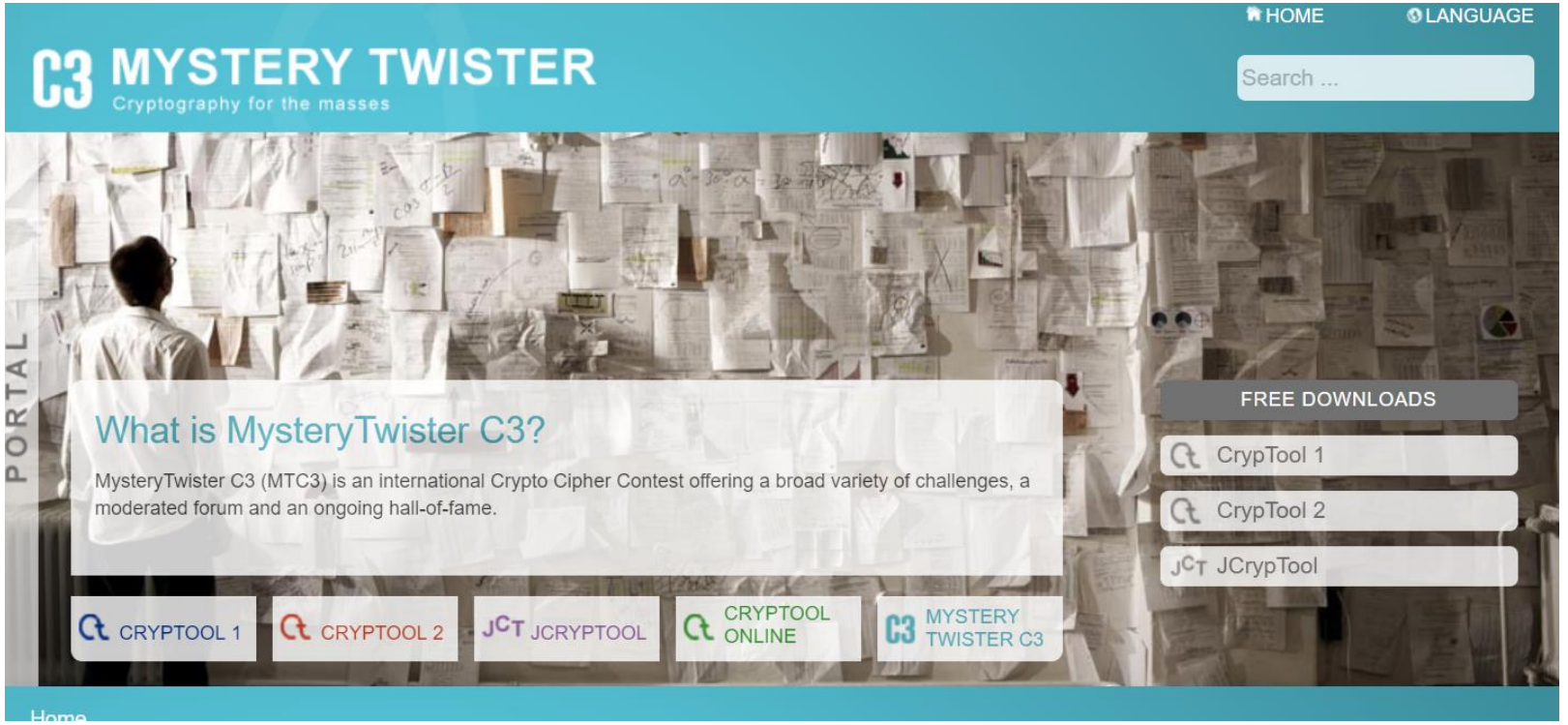


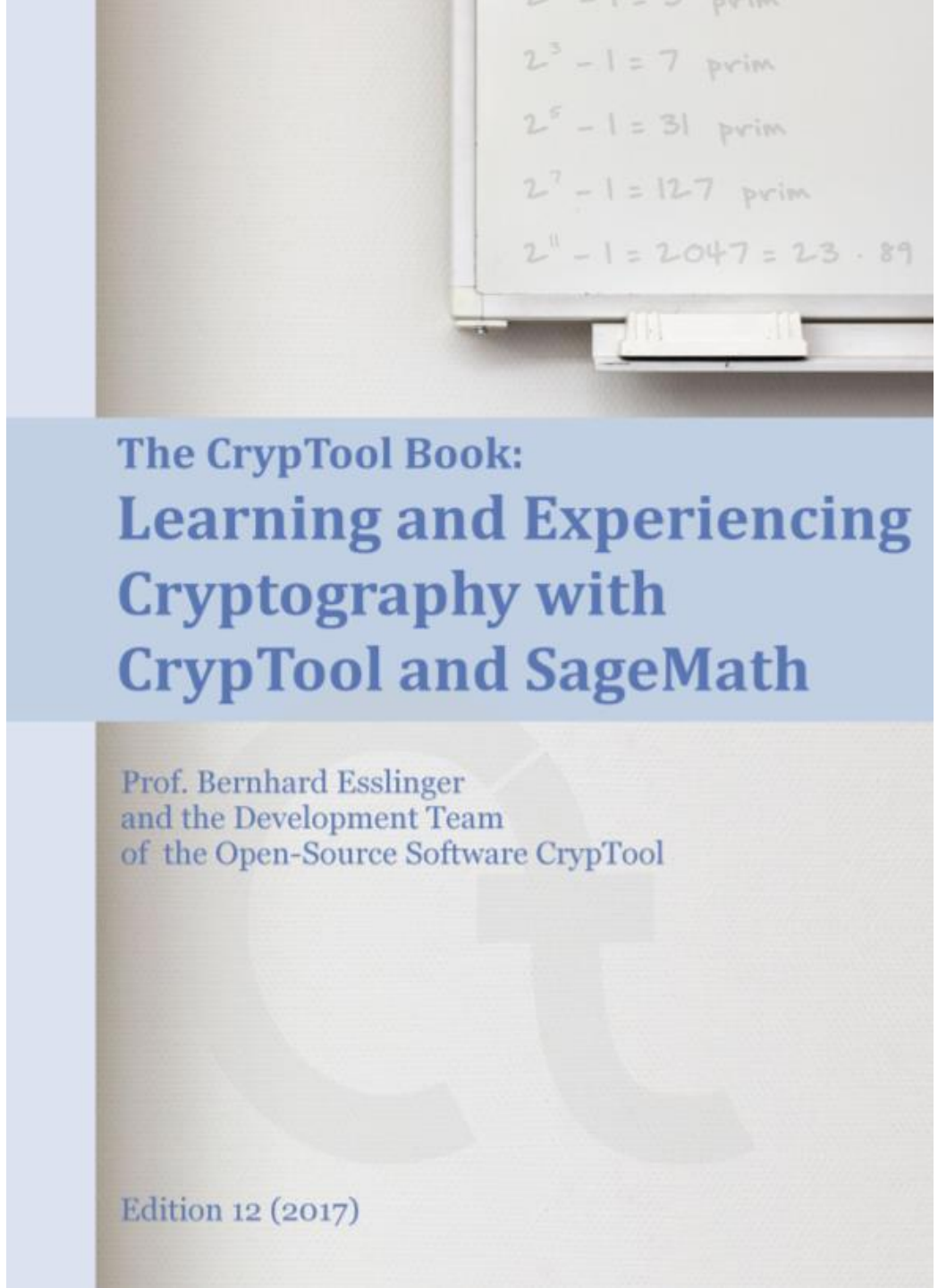
Mystery Twister C3 is an international Crypto Cipher Contest offering more than 200 challenges, a moderated forum and an ongoing hall-of-fame.

Mystery Twister C3 is available in English and German

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST





The **CrypTool Portal** -> **Documentation**

CT Book

CT Presentations

Some International Awards

2004 TeleTrusT (TTT Förderpreis / Sponsorship Award)

2004 NRW (IT Security Award NRW)

2004 RSA Europe (Finalist of European Information Security Award 2004)

2008 “Selected Landmark” in initiative “Germany – Land of Ideas”

CrypTool in scientific papers

Teaching Cryptology At All Levels Using CrypTool R.Yang, L. Wallace, I. Burchett Proceedings of the 15th Colloquium for information Systems Security Education Fairborn, Ohio June13-15, 2011

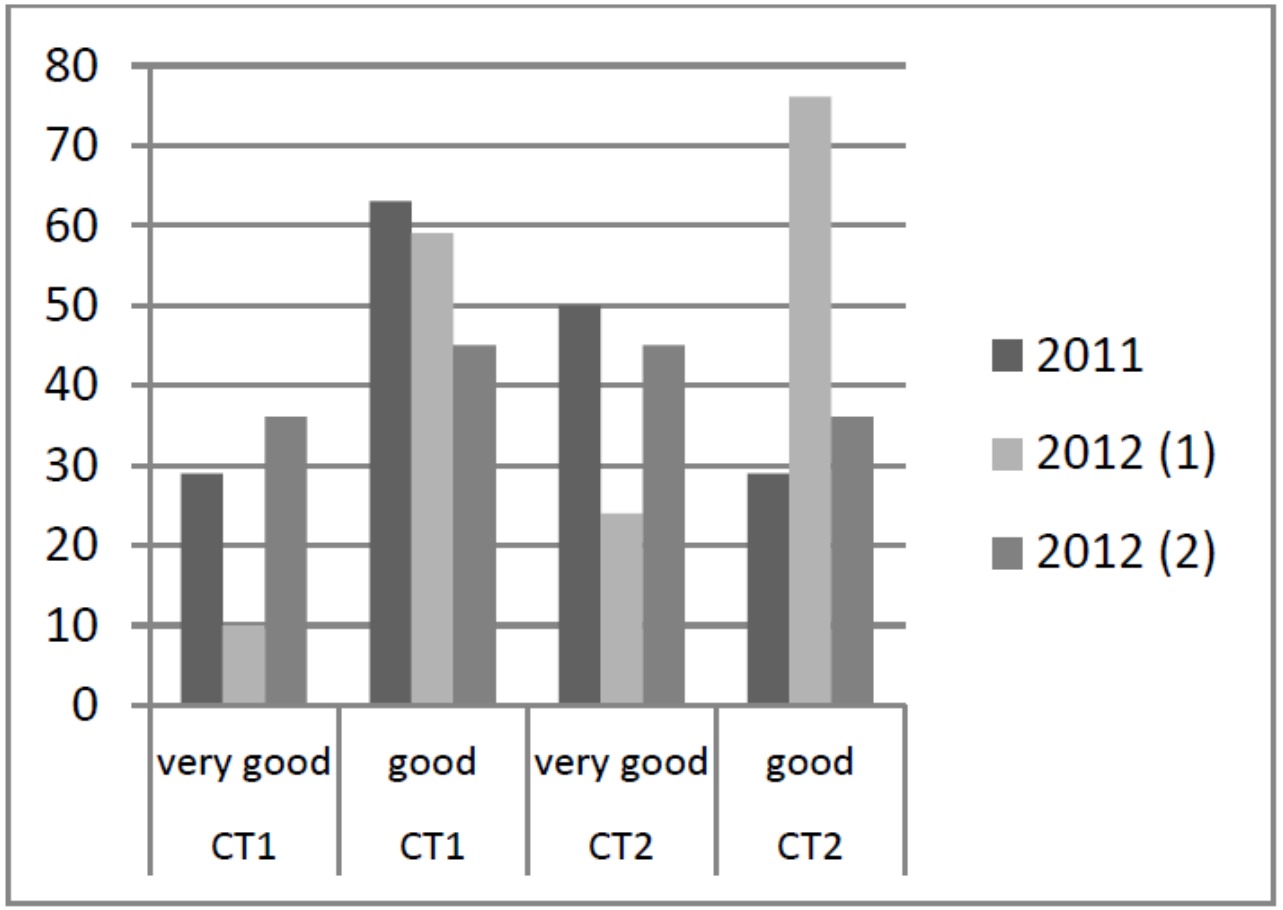
An Interactive and Collaborative Approach to Teaching Cryptology S. Adamovic , M.Sarac , M.Veinovic , M. Milosavljevic and A.Jevremovic *Journal of Educational Technology & Society* Vol. 17, No. 1, Game Based Learning for 21st Century Transferable Skills: Challenges and Opportunities (January 2014), pp. 197-205

Cryptool 2 in Teaching Cryptography Major K.Loussios *Journal of Computations & Modelling*, vol.4, no.1, 2014, 349-358 ISSN: 1792-7625 (print), 1792-8850 (online) Scienpress Ltd, 2014

Visualization of the Avalanche Effect in CT2, Camilo Echeverri *Thesis Bachelor of Science Wirtschaftsinformatik*

Reducing the complexity of understanding cryptology using CrypTool, S. Hick, B. Esslinger, and A.Waker

Usability of Cryptool



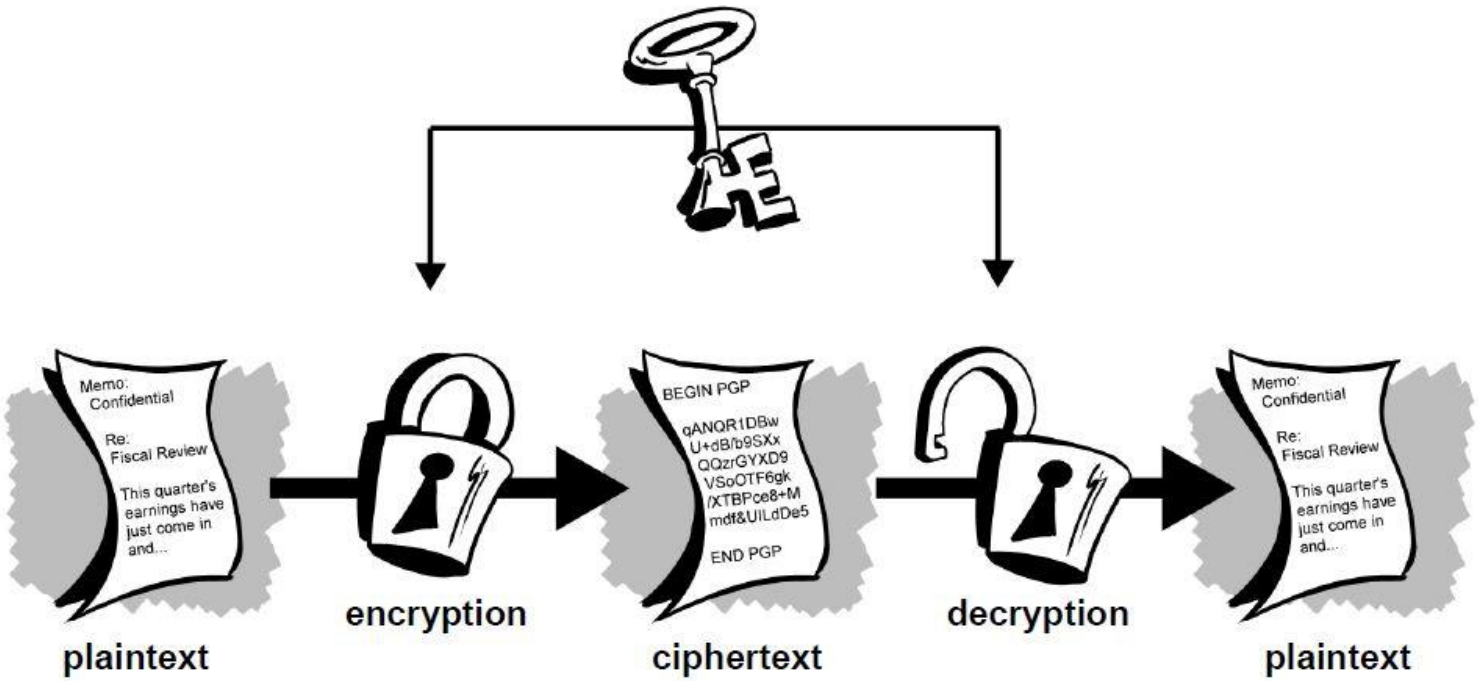
Event “Schuelerkrypto” (Student Crypto) in Germany

Reducing the complexity of understanding cryptology using CrypTool, S. Hick, B. Esslinger, and A.Waker

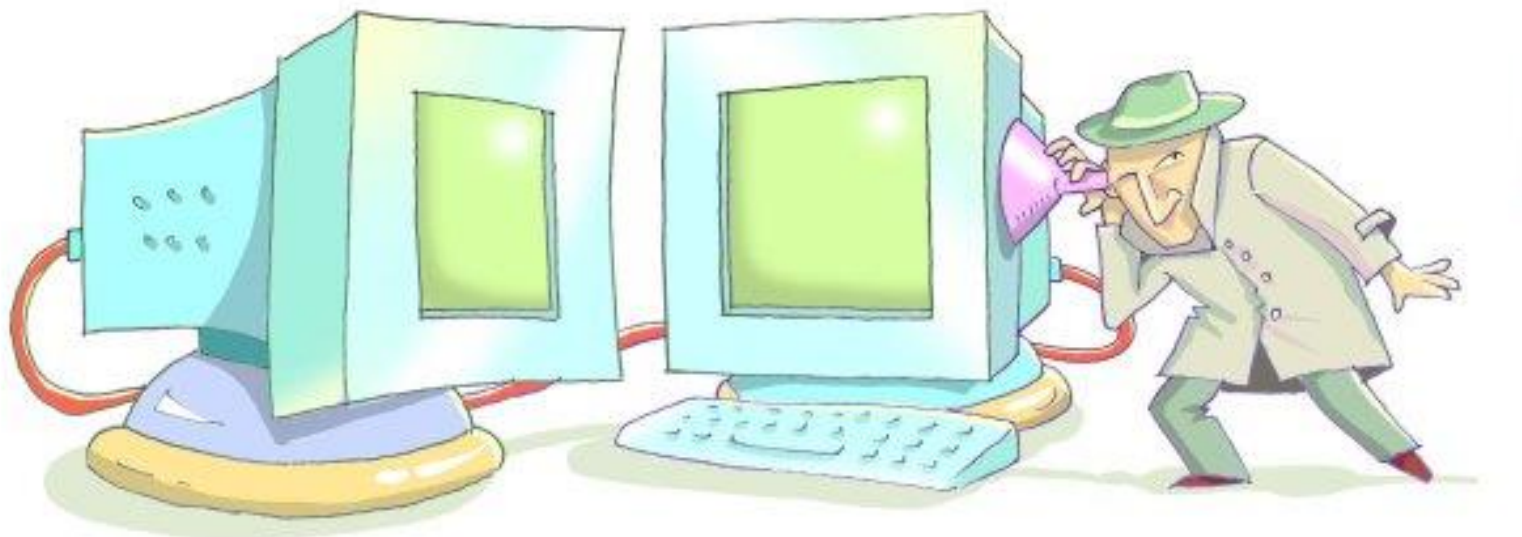
The 10th International Conference on Education and Information Systems,Technologies and Applications (EISTA 2012), Orlando, Florida, USA, (17-20 July 2012)

Classical Cipher

A **cipher** is the set of instructions for encrypting or decrypting a message



Cryptanalysis: science of studying attacks against cyphertexts.



Classical Cyphers

A **classical cipher** was used from 2000 B.C. in Egypt to World War II, before computers become available.

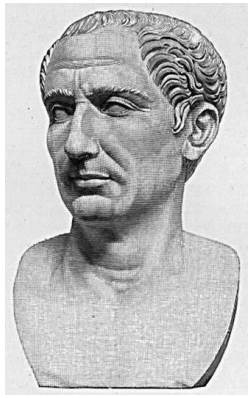
.

Plaintext is viewed as a sequence of elements (e.g., bits or characters)

Substitution cipher: replacing each element of the plaintext with another element (Caesar, Vigenère, Hill).

Transposition (or permutation) cipher: rearranging the order of the elements of the plaintext (Scytale, Rail fence).

Product cipher: using multiple stages of substitutions and transpositions (ADFG(V)X).



Caesar Cipher

Caesar cipher is a type of **substitution** cipher in which each letter in the plaintext is replaced by a letter some fixed number (**Key**) of positions down the alphabet.

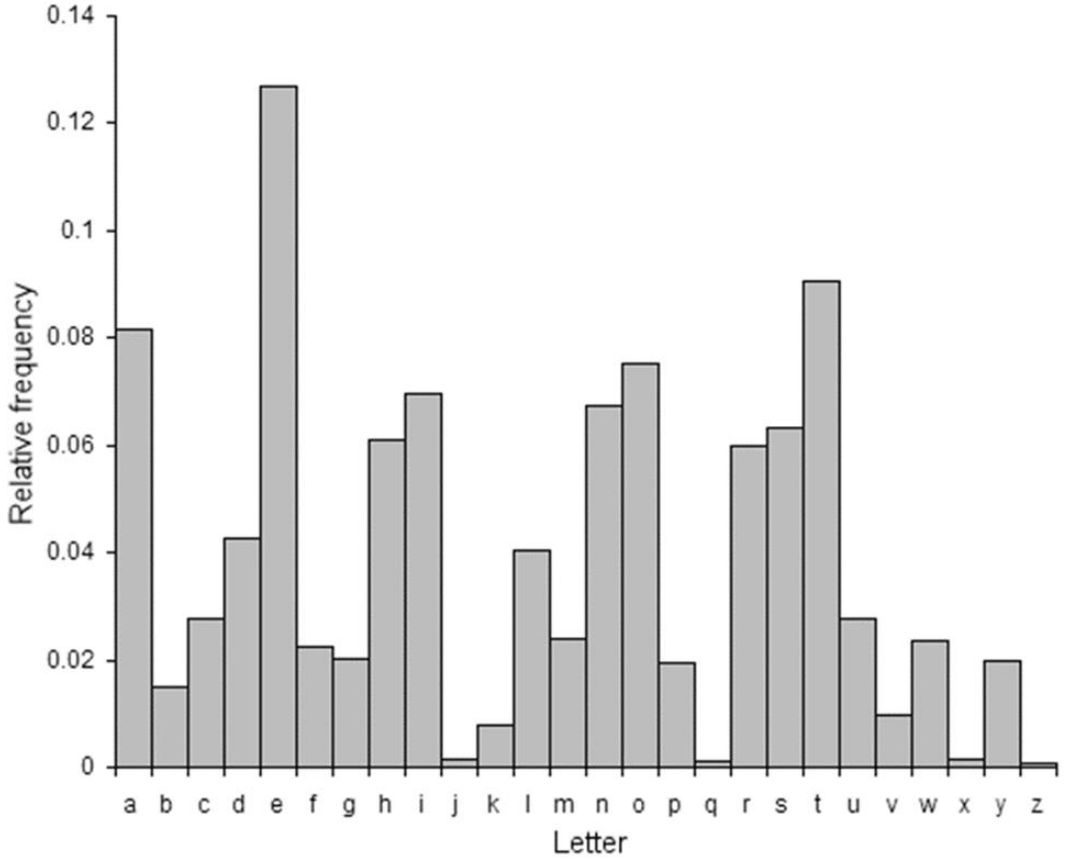
Monoalphabetic cipher: fixed substitution over the entire message

Cipher Wheel

Cryptanalysis of the Caesar Cipher

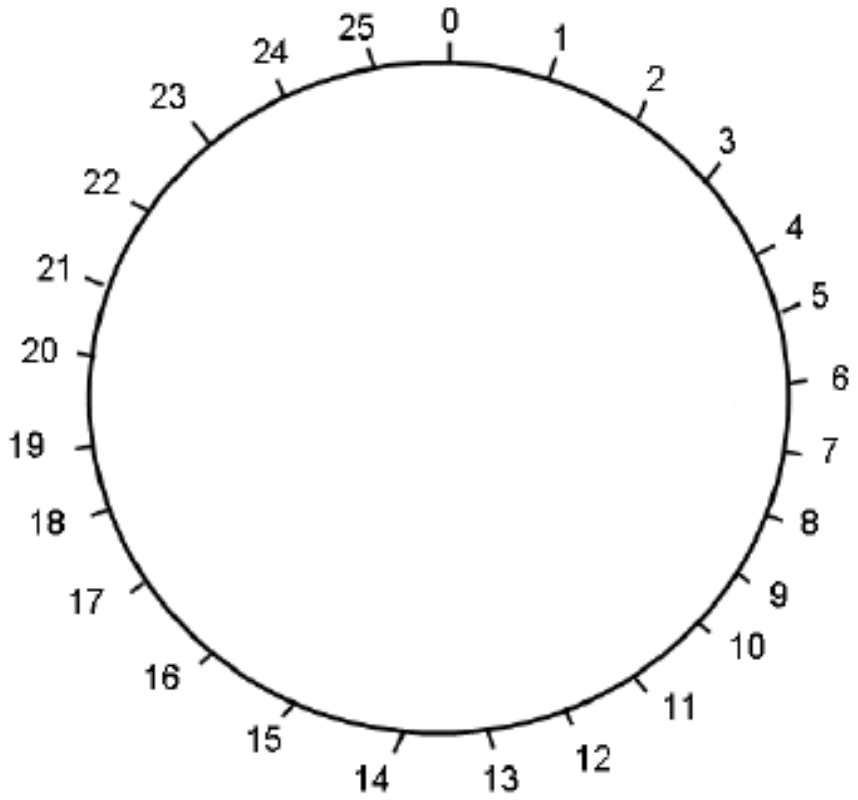
Brute-Force Attack: only 26 possible keys

Character Frequencies:



Letter Frequency for English Letters

Modular (Clock) Arithmetic



$12 \equiv 12 \bmod 26$

$27 \equiv 1 \bmod 26$

$53 \equiv 1 \bmod 26$

$-1 \equiv 25 \bmod 26$

Vigenère Cipher

Vigenère Cipher is a **polyalphabetic** substitution first published in 1585 **.**

To encrypt, a table of alphabets can be used, called a *tabula recta* or *Vigenère square*, that consists of several Caesar ciphers in sequence with different shift values.

A **keyword** is then used to choose which ciphertext alphabet to use.

The Vigenère square

	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

Cryptanalysis of Vigenère Cipher

Kasiski Method (1863): use repetitions in ciphertext to give clues about the length of the keyword, looking for same plaintext an exact period apart, leading to same ciphertext.

Plaintext: TOBEORNOTTOBE
Key: NOWNOWNOWNOWN
Ciphertext: GCXRCNACPGCXR

Since repeats are 9 chars apart, guess period is 3 or 9

The Friedman test (1920): uses the index of coincidence, The Incidence of Coincidence is the probability that two randomly selected letters are the same. i.e. it measures variation of the cipher letter frequencies.

Solving Vigenère Cipher:

1. Use Kasiski method & IC to estimate the length of the key word, d.

2. Separate ciphertext into d sections, and solve each as a monoalphabetic cipher.

Hill cipher

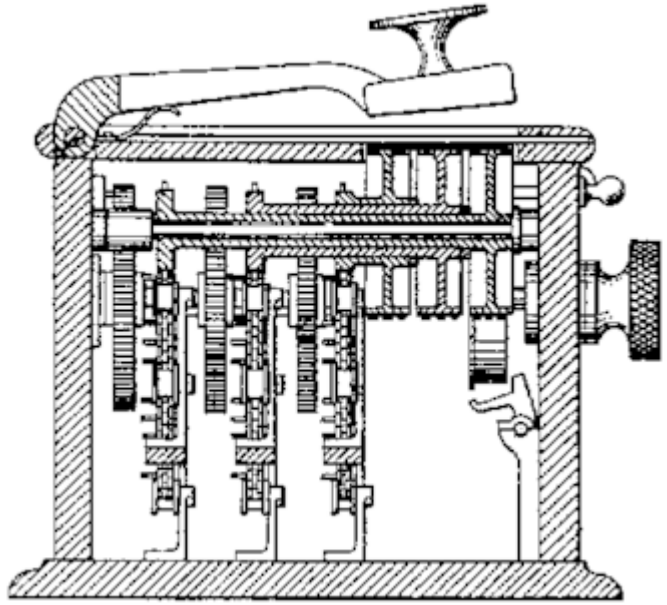
Hill cipher is **a polygraphic substitution** cipher based on linear algebra (1929).

Key: Invertible *n* × *n* matrix -> gcd (d,26)=1

Plaintext and Ciphertext*: n x m* matrix

$$C \equiv Key * P \pmod{26}$$

$$P \equiv Key^{-1} * C \pmod{26}$$



Hill's cipher machine which performed a 6 × 6 matrix multiplication modulo 26 using a system of gears and chains.

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

$$I_{2x2} = \begin{pmatrix} 1 & 24 \\ 18 & 17 \end{pmatrix}$$

d=11

gcd (26,d)=1

P = **CRYPTOOL**

$$P = \begin{pmatrix} C & Y & T & O \\ R & P & O & L \end{pmatrix} = \begin{pmatrix} 2 & 24 & 19 & 14 \\ 17 & 15 & 14 & 11 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 24 \\ 18 & 17 \end{pmatrix} * \begin{pmatrix} 2 & 24 & 19 & 14 \\ 17 & 15 & 14 & 11 \end{pmatrix} = \begin{pmatrix} 410 & 384 & 355 & 278 \\ 325 & 687 & 580 & 439 \end{pmatrix} \equiv \begin{pmatrix} 20 & 20 & 17 & 18 \\ 13 & 11 & 8 & 23 \end{pmatrix} MOD\ 26$$

$$C = \begin{pmatrix} U & U & R & S \\ N & L & I & X \end{pmatrix} = UNULRISX$$

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

$$I_{2x2}^{-1} \equiv \begin{pmatrix} 17 & 2 \\ 8 & 1 \end{pmatrix} \text{MOD } 26$$

$$P = \begin{pmatrix} 17 & 2 \\ 8 & 1 \end{pmatrix} * \begin{pmatrix} 20 & 20 & 17 & 18 \\ 13 & 11 & 8 & 23 \end{pmatrix} = \begin{pmatrix} 2 & 24 & 19 & 144 \\ 17 & 15 & 14 & 11 \end{pmatrix} MOD\ 26$$

$$P = \begin{pmatrix} C & Y & T & O \\ R & P & O & L \end{pmatrix} = \text{CRYPTOOL}$$

Cryptanalysis of Hill Cipher

known plaintext – ciphertext: the key can be recovered solving a system of linear equations

$C \equiv Key * P \pmod{26}$

$$\begin{pmatrix} 20 & 20 & 17 & 18 \\ 13 & 11 & 8 & 23 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} 2 & 24 & 19 & 14 \\ 17 & 15 & 14 & 11 \end{pmatrix}$$

$$2a + 17b = 20$$
$$\vdots$$

frequency analysis: for very long ciphertexts, frequency analysis may be useful when applied to bigrams (for a 2 by 2 hill cipher)

The most common English digraphs in order of frequency:
TH, HE, AN, IN, ER, ON, RE, ED, ND, HA, AT, EN, ES, OF, NT, EA, TI, TO, IO, LE, IS, OU, AR, AS, DE, RT, VE

N-Gram List of Hill encryption of <startingexample-en>, key <DIM 2, KEY: BY SR , ALPHABET: ABC...

Selection
- Histogram (26)
- Digram (270)
- Trigram (357)
- 4 -gram (303)

No.	Character seq...	Frequency in %	Frequency
1	EH	1.8450	10
2	OL	1.8450	10
3	HW	1.4760	8
4	IB	1.4760	8
5	SD	1.4760	8
6	LO	1.2915	7
7	RI	1.2915	7

$$C \equiv Key * P \pmod{26}$$

Guess: $\begin{pmatrix} 4 & 14 \\ 7 & 11 \end{pmatrix} = Key * \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} MOD\ 26$

$$P^{-1} = \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix}$$

$$Key = \begin{pmatrix} 4 & 14 \\ 7 & 11 \end{pmatrix} * \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \text{ MOD } 26 \ ?$$

If it is not, try other combinations of common ciphertext digrams until we get something that is correct.

$$\begin{pmatrix} t \\ h \end{pmatrix} \rightarrow \begin{pmatrix} f \\ t \end{pmatrix} \qquad \begin{pmatrix} h \\ e \end{pmatrix} \rightarrow \begin{pmatrix} z \\ m \end{pmatrix}$$

$$\begin{pmatrix} 19 \\ 7 \end{pmatrix} \rightarrow \begin{pmatrix} 5 \\ 19 \end{pmatrix} \qquad \begin{pmatrix} 7 \\ 4 \end{pmatrix} \rightarrow \begin{pmatrix} 25 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 25 \\ 19 & 12 \end{pmatrix} = Key * \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} MOD\ 26 \qquad P^{-1} = \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix}$$

$$Key = \begin{pmatrix} 5 & 25 \\ 19 & 12 \end{pmatrix} * \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 18 & 17 \end{pmatrix} \text{MOD } 26$$