Sicherheit in Kommunikationsnetzen
(Network Security)

Historic Ciphers

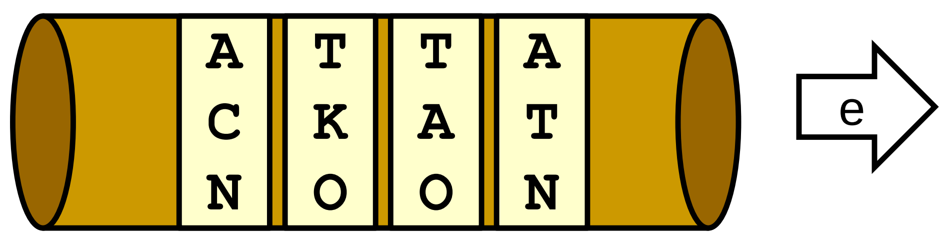
Dr.-Ing. Matthäus Wander

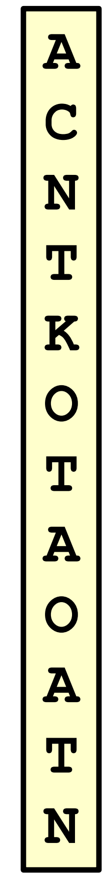
Universität Duisburg-Essen

Skytale

- Skytale: cipher used in Sparta around 500 BC
- Wooden baton („Holzstab“)
  - Wrapped with parchment or leather
  - Write message horizontally (around whole baton)
  - Unwrap leather ⇨ characters scrambled
  - Wrap again ⇨ message becomes readable

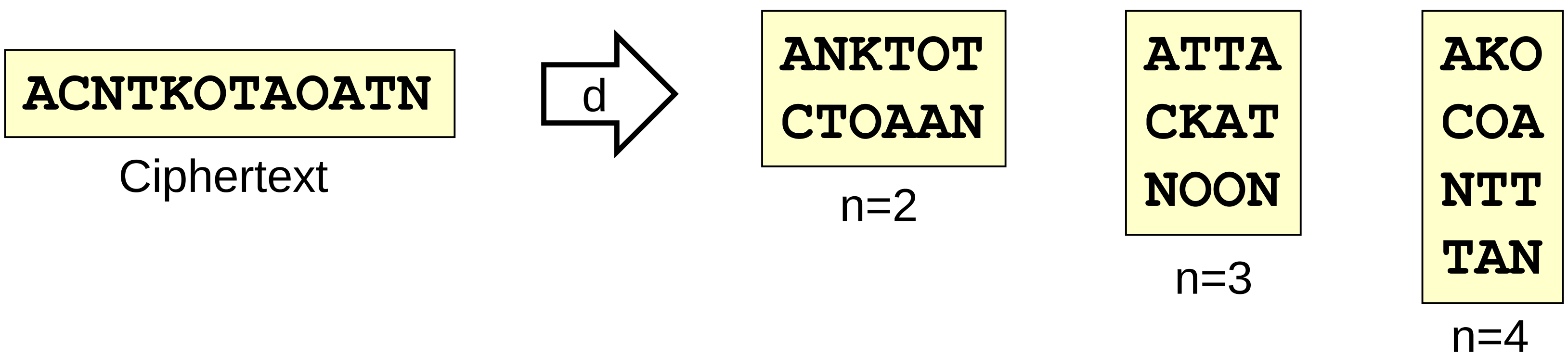
Source: Wikimedia Commons





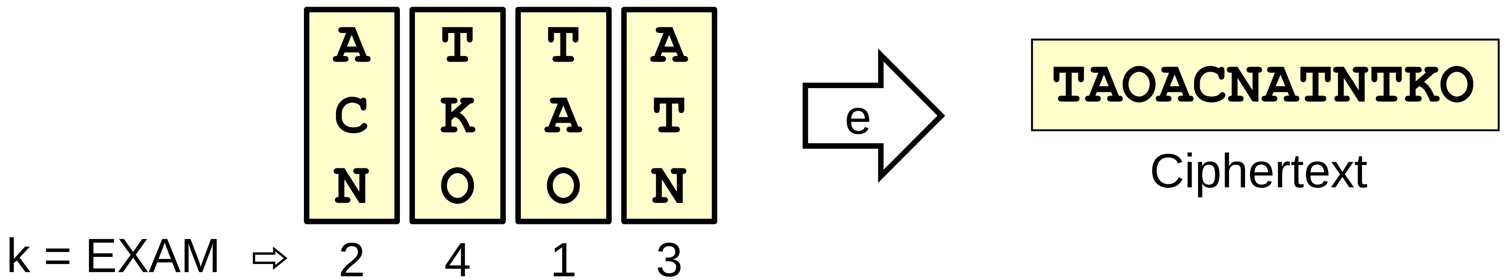
Skytale (2)

- Secret key: radius of baton
  - Key space: with message length *n*, there are *n* possibilities for how many characters fit into a column
- Cryptanalysis: try all *n* possibilities
  - Brute-force attack of cost O(*n*)
- Kerckhoffs‘ principle satisfied by Skytale?



Transposition Ciphers

- Skytale is a transposition cipher
  - Shift characters of plaintext message
  - The original characters are not replaced, only moved
  - Ciphertext is a permutation of the plaintext
- Other ciphers have different transposition rules
  - Columnar transposition re-orders columns
  - Key: column length and order (given by keyword)



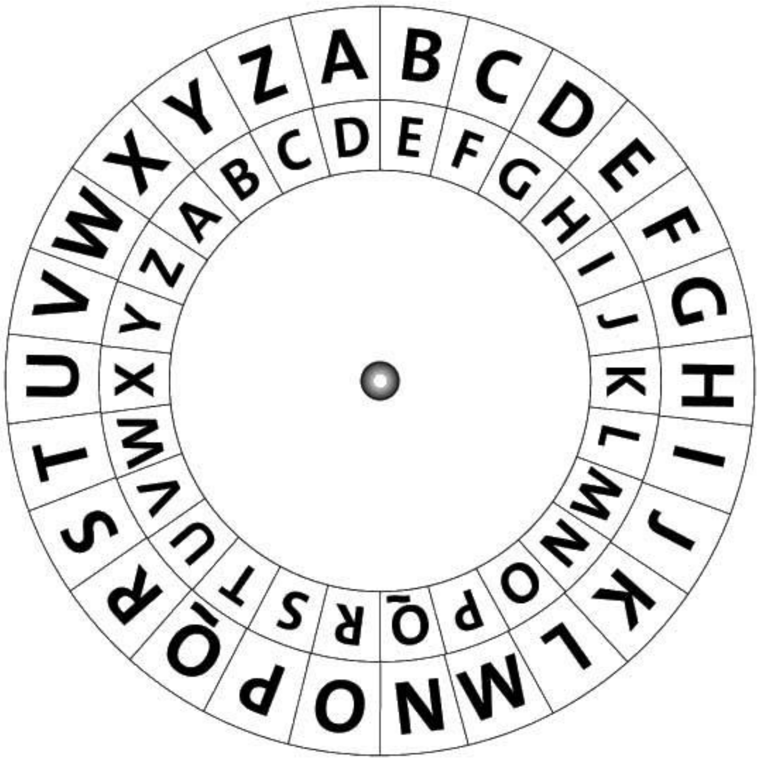
Caesar Cipher

- Caesar cipher used by Julius Caesar (100–44 BC)
- Maps plaintext onto ciphertext alphabet
  - Alphabets are shifted against each other
  - Secret key: shift offset

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
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

- Encryption: $e_{k=3}$(„ATTACK“) = „DWWDFN“
- Decryption: inverse mapping of alphabets

Cipher Disk



Source:
https://tex.stackexchange.com/questions/103364/how-to-create-a-caesars-encryption-disk-using-latex

Source:
CryptoMuseum.com

Shift Ciphers

- Special case: $e_{13}(e_{13}(m))=m$ (self-inverse)
  - Identical en-/decryption function (known as ROT13)
  - Used to “scramble” text, e.g. in discussion boards
- Caesar is a shift cipher or additive cipher:
  - Enumerate alphabet: A=0, B=1, C=2, …, Z=25
  - $e_k(m) \equiv m + k \bmod |\mathcal{A}|$ where $\mathcal{A}$ is the alphabet
  - $d_k(c) \equiv c - k \bmod |\mathcal{A}|$ e.g. $|\mathcal{A}|=26$
- Cryptanalysis: try all shift offsets
  - Brute-force attack of cost $|\mathcal{A}|=|\mathcal{K}|=26$

Monoalphabetic Ciphers

- Shift ciphers substitute character with another
- Problem: key space is too small
- Idea: use arbitrary mapping between alphabets
  - Keyword: „WOW SUCH SECRET VERY HIDDEN"
  - Eliminate double characters: „WOSUCHERTVYIDN"
  - Fill with remaining characters from 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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
W	O	S	U	C	H	E	R	T	V	Y	I	D	N	A	B	F	G	J	K	L	M	P	Q	X	Z

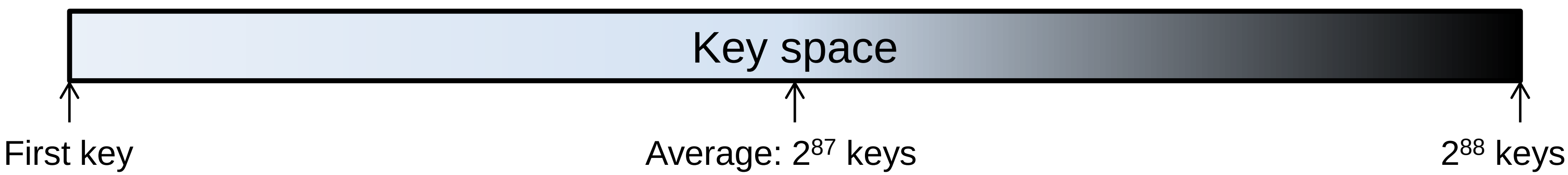
Monoalphabetic Ciphers: Cryptanalysis

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

- How large is the key space $\mathcal{K}$?
  - We can use any keyword of up to $|\mathcal{A}|=26$ characters
  - We map A→{A,…,Z}: 26 possibilities
  - We map B→{A,…,Z} except for {W}: 25 possibilities
  - We map C→{A,…,Z} except for {W, O}: 24 possibilities
- Total: $26 \times 25 \times 24 \times \ldots \times 1 = 26! \approx 4 \times 10^{26} \approx 2^{88}$

Brute-Force Attack

- Modern CPUs perform around 10^{11} to 10^{12} instructions per sec (Dhrystone benchmark)
- Assume attacker checks 10^{12} keys per second
  - $10^{26} / 10^{12} = 10^{14}$ seconds to exhaust all keys $\approx$3 million years



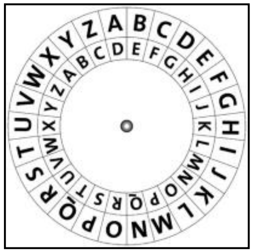
  - Attacker may find key on first or last decrypt attempt
  - Average: after computing half of the key space ⇨ after $\approx$1.5 million years

Dictionary Attack

- Human-chosen keywords are easy to remember
  - e.g. „secret“, „letmein“ or „msvduisburg“
- A dictionary attack attempts decryption of words from a given list
  - Much faster than a brute-force attack, but not guaranteed to find the correct key
- Permute or transform words to find variants
  - e.g. „terces“, „letmein!“ or „msv02duisburg“
- Keys should be chosen randomly if memorization is not required

Statistical Analysis

- Monoalphabetic substitution maps a plaintext character to the same ciphertext character
  - Character positions do not change
  - Patterns or character frequencies are not hidden
- Plaintext is usually not random data
  - Natural languages have known grammar and letter frequencies
  - Images, audio etc. use file formats with partly known header information



Cipher.JPEG

```
00000000: FF D8 FF E0 00 10 4A 46|49 46 00 01 01 00 00 01  | ÿØÿà..JFIF......
00000010: 00 01 00 00 FF E2 0C 58|49 43 43 5F 50 52 4F 46  | ....ÿâ.XICC_PROF
```

Letter Frequency in English

- Non-uniform character distribution
  - „E“ is most frequent (12.7% instead of 1/26=3.8%)

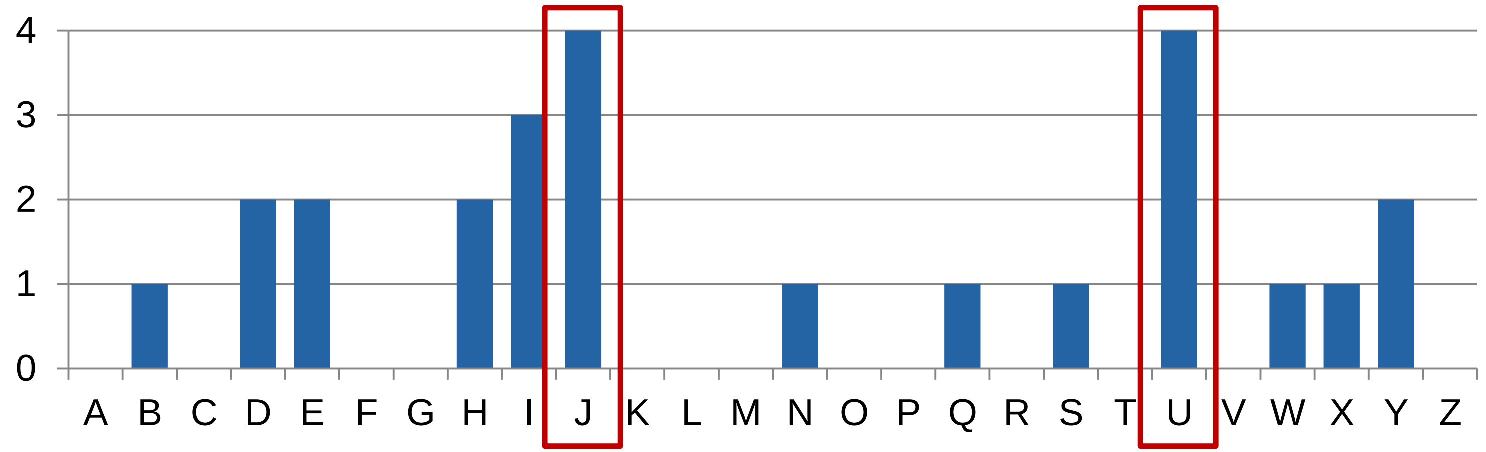
Letter	Relative frequency in the English language	Letter	Relative frequency in the English language
a	8.167%	n	6.749%
b	1.492%	o	7.507%
c	2.782%	p	1.929%
d	4.253%	q	0.095%
e	12.702%	r	5.987%
f	2.228%	s	6.327%
g	2.015%	t	9.056%
h	6.094%	u	2.758%
i	6.966%	v	0.978%
j	0.153%	w	2.360%
k	0.772%	x	0.150%
l	4.025%	y	1.974%
m	2.406%	z	0.074%

Statistical Analysis of Caesar Cipher

- Exploit character frequency in Caesar cipher
- We need:
  - Knowledge (or guess) of language being used
  - Character frequency (language statistics)
- Count character frequency in ciphertext
- Map most frequent ciphertext character to plaintext „E“ ⇨ best candidate for shift offset
  - Check whether frequency of other characters matches
  - If not: try second-best shift candidate

Statistical Analysis of Caesar Cipher (2)

- Example ciphertext (English):
  c=„**JXYI JUNJ YI DE BEDWUH Q IUSHUJ**“
- Histogram of character frequency:



- 2 key candidates: e_5(„E“)= „J“ or e_{16}(„E“)= „U“

Statistical Analysis of Caesar Cipher (3)

- Example ciphertext (English):
  c=„**JXYI JUNJ YI DE BEDWUH Q IUSHUJ**“
- Most frequent: „J“ and „U“ (4 times, 16%)
- Attempt:
  - $d_5(c)$ = „**ESTD EPIE TD YZ WZYRPC L DPNCPE**“
  - Letter frequencies in English: E (12.7%), P (2%)
- Attempt:
  - $d_{16}(c)$ = „**THIS TEXT IS NO LONGER A SECRET**“
  - Letter frequencies in English: E (12.7%), T (9%)

Attacking Monoalphabetic Ciphers

- Same principle for any monoalphabetic cipher
- Problem:
  - Can‘t map character frequencies 1:1 onto ciphertext alphabet due to statistical variations
  - Especially with short messages
- Idea:
  - Classify characters of similar frequency into groups
  - Narrow down possible character mappings
  - Use bigram (2-character sequence) or trigram frequency for further discrimination

Attacking Monoalphabetic Ciphers (2)

- Example: German
  - E and N are most frequent
    ⇨ we learn E, N
  - I, S, R, A, T have similar frequency

Letter	%	Letter	%
A	6.51	N	9.78
B	1.89	O	2.51
C	3.06	P	0.79
D	5.08	Q	0.02
E	17.40	R	7.00
F	1.66	S	7.27
G	3.01	T	6.15
H	4.76	U	4.35
I	7.55	V	0.67
J	0.27	W	1.89
K	1.21	X	0.03
L	3.44	Y	0.04
M	2.53	Z	1.13

Attacking Monoalphabetic Ciphers (3)

- Group characters of similar frequency
  - Assign ciphertext characters to groups

Group	Total %
E, N	27.18
I, S, R, A, T	34.48
D, H, U, L, C, G, M, O, B, W, F, K, Z	36.52
P, V, J, Y, X, Q	1.82

Letter	%	Letter	%
A	6.51	N	9.78
B	1.89	O	2.51
C	3.06	P	0.79
D	5.08	Q	0.02
E	17.40	R	7.00
F	1.66	S	7.27
G	3.01	T	6.15
H	4.76	U	4.35
I	7.55	V	0.67
J	0.27	W	1.89
K	1.21	X	0.03
L	3.44	Y	0.04
M	2.53	Z	1.13

Attacking Monoalphabetic Ciphers (4)

- We know E and N
- We know 5 chars are {I, S, R, A, T} but not exactly which ones

Group	Total %
E, N	27.18
I, S, R, A, T	34.48
D, H, U, L, C, G, M, O, B, W, F, K, Z	36.52
P, V, J, Y, X, Q	1.82

Letter	%	Letter	%
A	6.51	N	9.78
B	1.89	O	2.51
C	3.06	P	0.79
D	5.08	Q	0.02
E	17.40	R	7.00
F	1.66	S	7.27
G	3.01	T	6.15
H	4.76	U	4.35
I	7.55	V	0.67
J	0.27	W	1.89
K	1.21	X	0.03
L	3.44	Y	0.04
M	2.53	Z	1.13

Attacking Monoalphabetic Ciphers (5)

- Analyze bigram statistics in ciphertext
  - EN is a frequent bigram in German (but NE is not)
  - Both single characters E and N are frequent
  - ⇨ Validates our classification of E and N

Group	Total %
E, N	27.18
I, S, R, A, T	34.48
D, H, U, L, C, G, M, O, B, W, F, K, Z	36.52
P, V, J, Y, X, Q	1.82

Bigram	%	Bigram	%
EN	3.88	ND	1.99
ER	3.75	EI	1.88
CH	2.75	IE	1.79
TE	2.26	IN	1.67
DE	2.00	ES	1.52

Attacking Monoalphabetic Ciphers (6)

- Identify single characters from bigrams
  - EI and inverse IE have similar frequency ⇨ we learn I
  - CH is frequent, but not HC nor the single chars ⇨ C, H
  - Continue learning characters, guess remaining ones

Group	Total %
E, N	27.18
I, S, R, A, T	34.48
D, H, U, L, C, G, M, O, B, W, F, K, Z	36.52
P, V, J, Y, X, Q	1.82

Bigram	%	Bigram	%
EN	3.88	ND	1.99
ER	3.75	EI	1.88
CH	2.75	IE	1.79
TE	2.26	IN	1.67
DE	2.00	ES	1.52

Recovering Plaintext

- We recover most characters, though we might misclassify some
  - Minor mistakes can be corrected like spelling errors
- We don‘t need 100% of a plaintext to deduce its information
  - **`I_ Deuts_hen re_raesentieren die _ehn haeu_i_sten _u_hsta_en drei _ierte_ eines Te_ts`**
  - **`In En__ish the ten _ost _re__ent _hara_ters re_resent three __arters o_ a te_t`**

Homophonic Ciphers

- Problem: character frequencies leak information
- Idea: hide frequencies by mapping the plaintext characters onto multiple ciphertext characters
  - e.g. $\mathcal{A}_P$ = {A, …, Z} $\mathcal{A}_C$ = {1, 2, …, 100}
- If p ∈ $\mathcal{A}_P$ has a frequency of q_p in the plaintext, assign q_p random characters of $\mathcal{A}_C$ to p
  - e.g. let q_p = 6% for p=„T“
  - then p=„T“ maps onto: e(„T“) ∈ {4, 8, 15, 16, 23, 42}
- Result: uniform distribution of all ciphertext characters c ∈ $\mathcal{A}_C$

Homophonic Ciphers (2)

- Homophonic ciphers are immune against single-character statistical cryptanalysis
- But still vulnerable against bigram analysis
  - e.g. in German, „C“ is usually part of „CH“ or „CK“
  - e(„C“) $\in$ {6, 28, 80}
  - If cipher character 28 is followed by {7,23,24,47,89}, then this set represents plaintext „H“ and „K“
- Statistical analysis is still possible because the ciphertext leaks patterns of the plaintext
  - It‘s harder though: attacker needs more ciphertext

Vigenère

- Blaise de Vigenère (1523–1596) suggested a polyalphabetic substitution cipher
  - Based on work by Trithemius and Bellaso
- Idea: combine different monoalphabetic ciphers
- Same plaintext character maps to one of several ciphertext alphabets
  - Select ciphertext alphabet via keyword character
- Presumed to be secure until 19th century
  - *„Le Chiffre indéchiffrable"*

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

Vigenère Square

Plaintext character

Keyword character

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

Vigenère Square

Plaintext character

Keyword character

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

Vigenère Encryption

- Keyword: „**VENUS**"
  - Repeat periodically to match plaintext length
- Plain: **P O L Y A L P H A B E T I C**
- Key: **V E N U S V E N U S V E N U**
- Cipher: **K S Y S S G T U U T Z X V W**

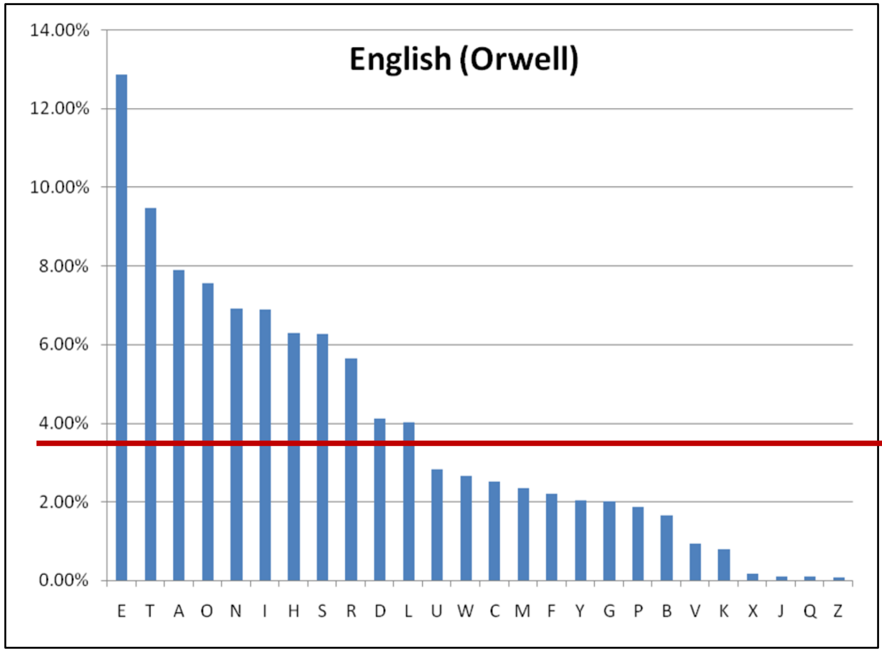
- Each key-letter represents one shift cipher
  - „A" + „S" → „S" and „B" + „S" → „T"

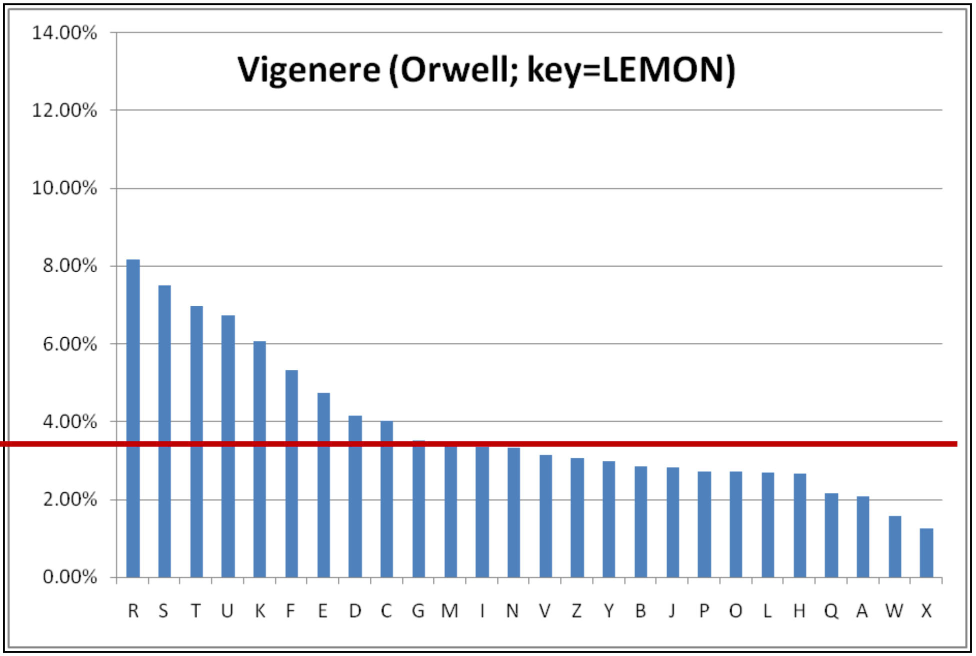
Vigenère Encryption (2)

- Same plaintext character may result in different ciphertext characters
  - „**ESSEN**“ twice in plaintext, but encoded differently
- Plain: **E S S E N B E I E S S E N I N**
- Key: **V E N U S V E N U S V E N U S**
- Cipher: **Z W F Y F W I V Y K N I A C F**
- Same ciphertext character may originate from different plaintext characters
  - Ciphertext „F“ represents plain „S“ or „N“

Cryptanalysis of Vigenère

- Vigenère still leaks some plaintext statistics
- Statistical analysis of book „1984“ (G. Orwell)
  - Uniform distribution should be 1/26=3.8% per char





Author: Derek Abbot (University of Adelaide)

Cryptanalysis of Vigenère (2)

- What if offset of plaintext and keyword match?
  - „**ESSEN**“ encoded twice as → „**ZWFYF**“
- Plain: **E S S E N K E N N T E S S E N**
- Key: **V E N U S V E N U S V E N U S**
- Cipher: **Z W F Y F F I A H L Z W F Y F**

- By observing repeating strings in the ciphertext, we can deduce the keyword length

Cryptanalysis of Vigenère (3)

- Kasiski's test: look for ciphertext repetitions
  - Published by Friedrich Kasiski in 1863
- Create list of repeating strings ≥ 3 chars
  - Problem: some repetitions may occur randomly
- Count distance between strings
  - Factorize distances and look for frequent primes
  - Key length is a frequent prime or a multiple thereof
- Cipher: **Z W F Y F F I A H L Z W F Y F**

distance: 10 = 2×5

Cryptanalysis of Vigenère (4)

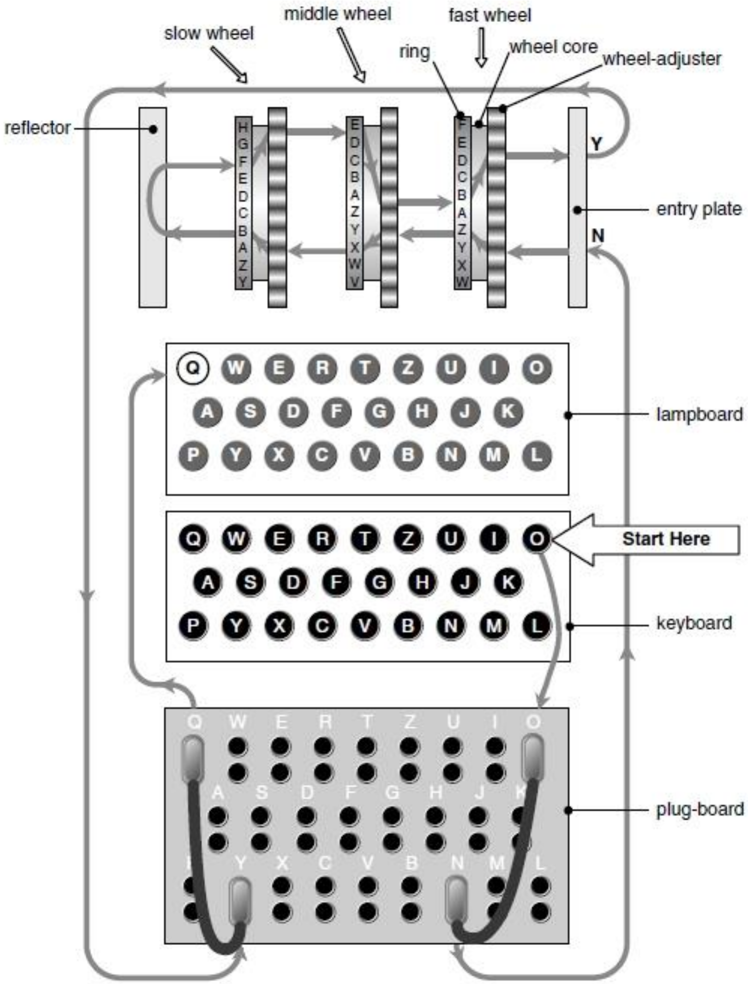
- Each keyword character is one shift cipher
  - We know how to cryptanalyze shift ciphers!

Plain:	E	S	S	E	N	K	E	N	N	T	E	S	S	E	N
Key:	V	E	N	U	S	V	E	N	U	S	V	E	N	U	S
Cipher:	Z	W	F	Y	F	F	I	A	H	L	Z	W	F	Y	F

- Statistical analysis of first cipher with ciphertext characters number 1, 6, 11, …
  - Analyze second cipher with characters 2, 7, 12, etc.
  - We will need longer messages for an attack, though

Enigma

Author: Alessandro Nassiri

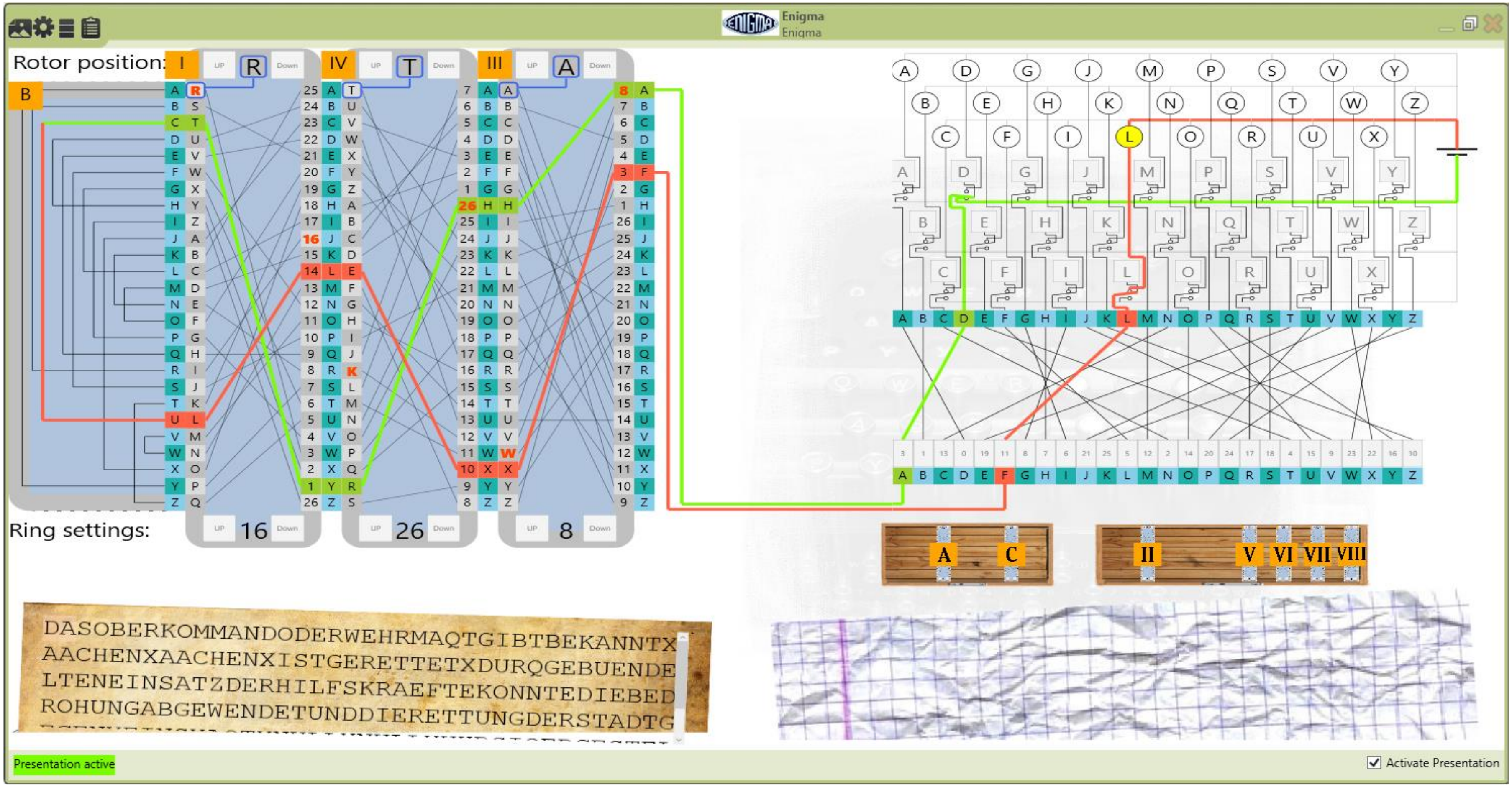


Author: Dustin A. Barrett

Enigma (2)

- Electromechanical rotor machine
  - Invented by Arthur Scherbius
  - Used by German Wehrmacht in World War II
- Keyboard input, letter lamps for output
- Multiple substitution stages form a polyalphabetic cipher
  - 3 rotor wheels, each a monoalphabetic substitution
  - Rotors move after each key press (configured by ring)
  - Plugboard for additional monoalphabetic substitution

Demo: Enigma (CrypTool 2)



Source: www.cryptool.org

Message Encryption and Transmission

- Each message is encrypted with individual key
  - Message key encrypted with daily key and prepended
- Ciphertext transmitted in Morse code over radio
  - Daily keys distributed in code books
  - „Kenngruppe“ identifies the recipient

Geheime Kommandosache!

Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

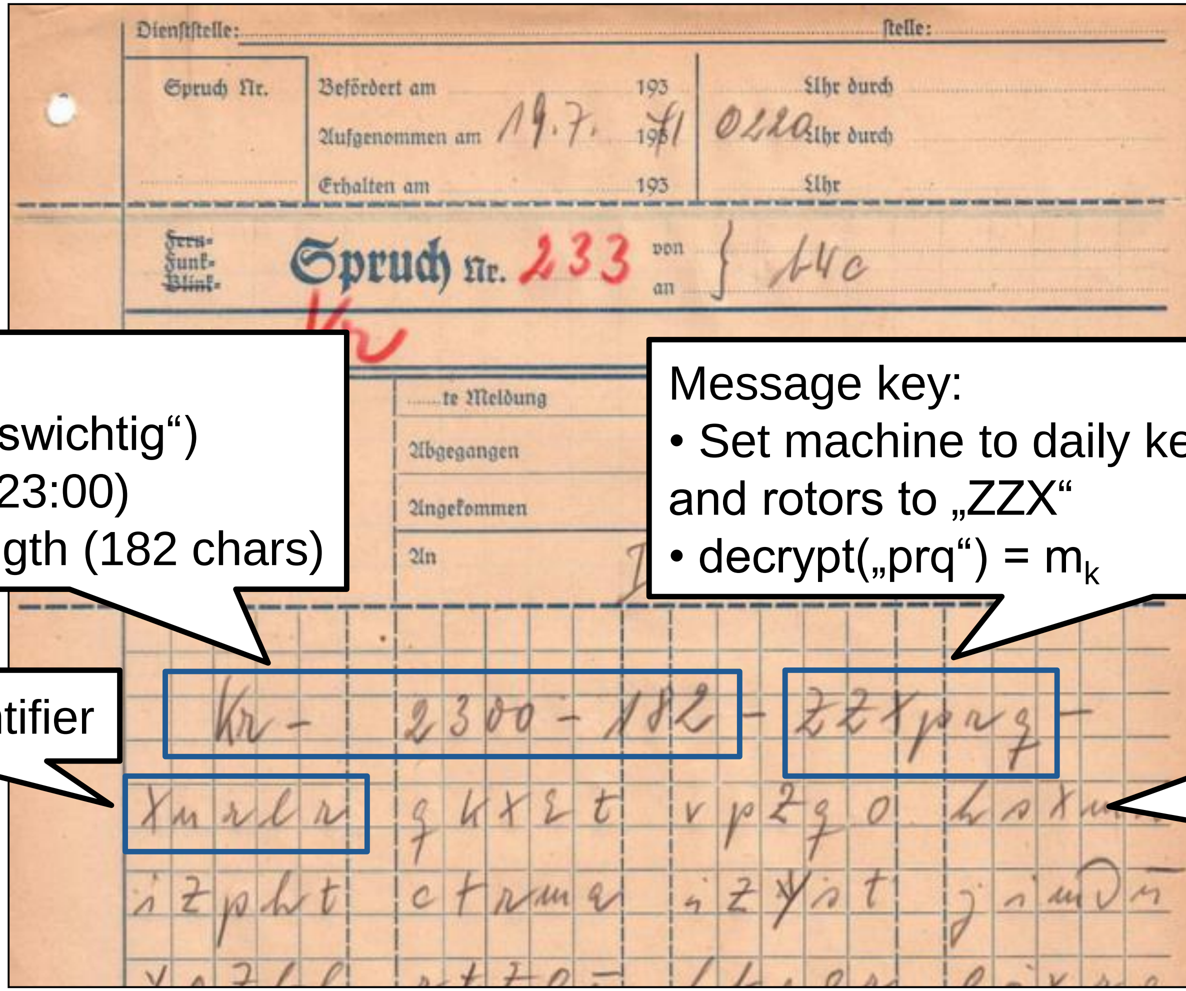
für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld

Source: Dirk Rijmenants

Example Message



Meta data:
- Flags („kriegswichtig")
- Timestamp (23:00)
- Message length (182 chars)

Message key:
- Set machine to daily key and rotors to „ZZX"
- decrypt(„prq") = m_k

Recipient identifier

Ciphertext:
- Decrypt with rotors set to m_k

Source: Frode Weierud (CryptoCellar.org)

Cryptanalysis of Enigma

- Size of key space $\mathcal{K}$?
- 3 out of 5 rotors, sequence without repetition
  - k–permutations of n: $\frac{n!}{(n-k)!} = \frac{5!}{(5-3)!} = 60$
- 26^3 initial rotor settings
- 26×26 ring settings (left ring irrelevant)
- Plugboard with e.g. 4 plugs: $\frac{1}{4!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2} \approx 5 \times 10^8$
  - Sum with 0 to 13 plugs $\approx 5 \times 10^{14}$
- Total: $|\mathcal{K}| \approx 3.8 \times 10^{23} \approx 2^{78}$

Cryptanalysis of Enigma (2)

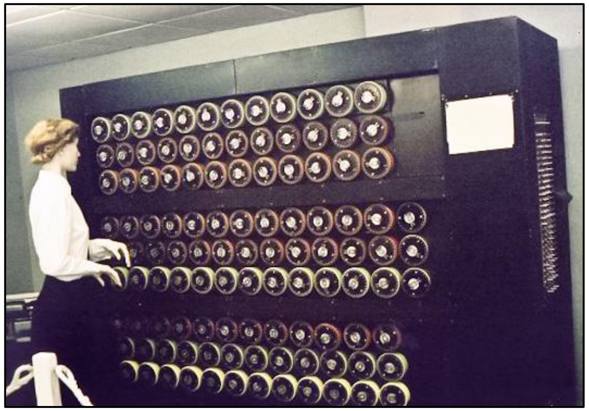
- Attack with letter statistics?
  - Polyalphabetic cipher is immune
- Attack with repeating cycles in ciphertext?
  - Ciphertext cycles only after 26^3 characters
- Weak spots
  - Encryption is self-inverse
  - A letter never maps to itself
- This limits the size of the key space and makes certain machine settings impossible

Attack Types

- What does the attacker know for cryptanalysis?
- Ciphertext-only attack
  - Only algorithm and ciphertext
- Known-plaintext attack
  - One or more pairs of plaintext + ciphertext
- Chosen-plaintext attack
  - Attacker can encrypt any plaintext message
- Chosen-ciphertext attack
  - Attacker can decrypt any ciphertext message

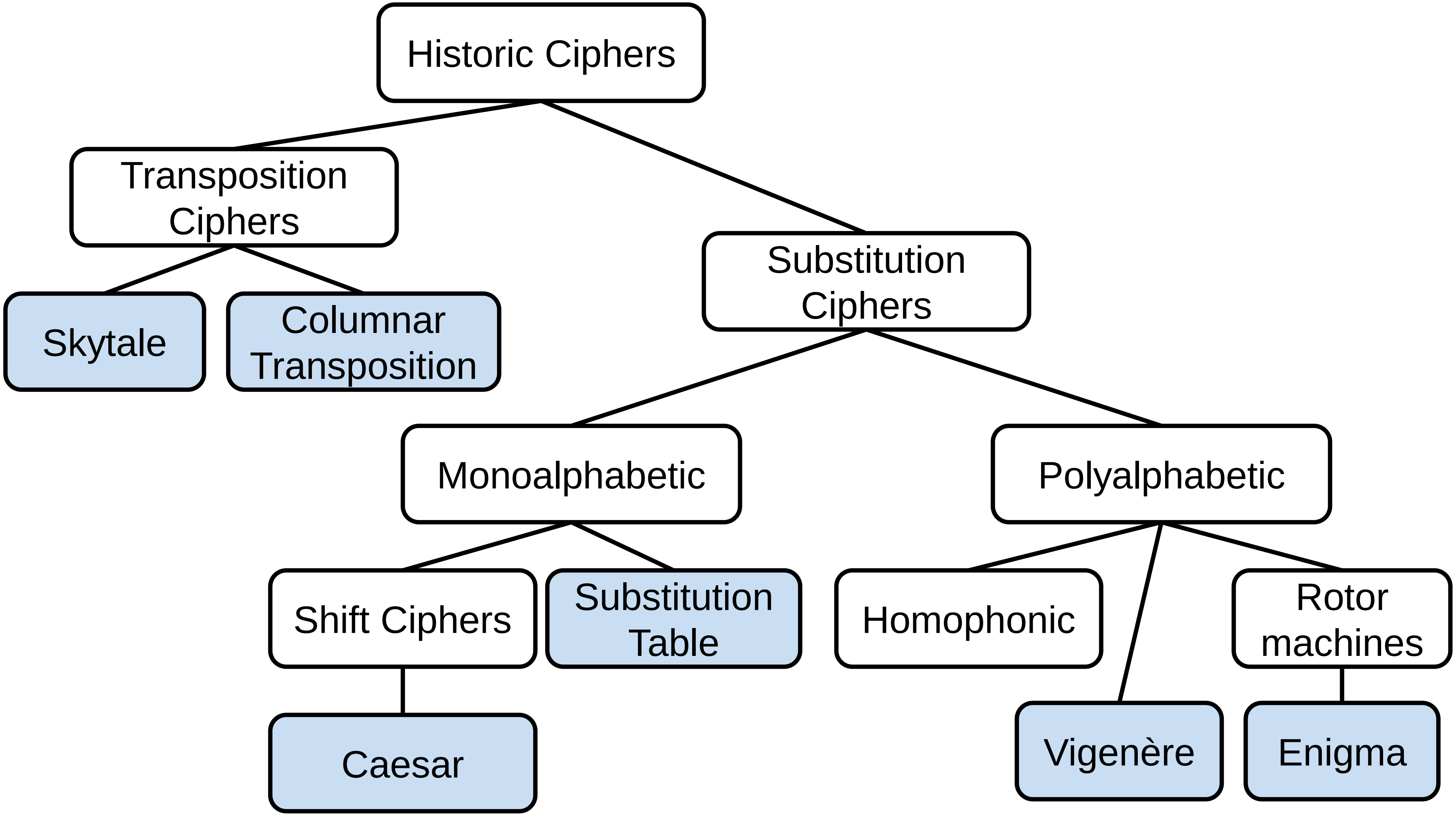
Cryptanalysis of Enigma (3)

- Messages contained phrases like „**WETTER**“
- British intelligence collected ciphertexts and gained knowledge of parts of plaintext (cribs)
- The Turing Bombe runs a crib-based brute-force attack to rule out impossible settings
  - Created by Alan Turing based on Marian Rejewski‘s Bomba
  - This narrows down possible daily keys within hours
  - But must be repeated every day



Author: Sarah Hartwell

Overview of Historic Cipher Classes



Historic Timeline

- 500 BC: Skytale
- 150 BC: Polybius square
- 50 BC: Caesar cipher
- 14th century: cryptanalysis by Arab scholars
- 15–16th century: polyalphabetic ciphers
  - Homophonic ciphers, Alberti cipher disk, Vigenère cipher
- 1917: Zimmermann telegram deciphered
- 1920–1970: rotor machines

Historic Timeline

- 1975: Data Encryption Standard (DES)
- Discovery of Public-Key Cryptography
  - 1976: Diffie-Hellman key exchange
  - 1978: Digital signatures by Rivest, Shamir, Adleman
- 1990s: encryption becomes mainstream
  - Crypto Wars on publicly accessible cryptography
- 1991: Pretty Good Privacy (PGP)
- 1996: SSL 3.0, became later TLS
- 2001: Advanced Encryption Standard (AES)

Conclusions

- Basic encryption methods: substitution and transposition
- Ciphers with small key space don‘t comply with Kerckhoffs‘ principle
  - But a large key space is not necessarily secure either
  - Keys should be chosen randomly
- Cryptanalysis exploits patterns and structure of the plaintext that leaks to the ciphertext
  - Multiple encryption stages increase the security