Historical ciphers II

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Playfair cipher – keyword expansion

- The Playfair cipher uses a keyword.
- Encryption/decryption uses a 5×5 grid of letters.
- Turn the keyword into this grid by filling in the letters of the keyword row-wise from the top left corner.
  The grid contains each letter once, with I and J identified; so when you reach a letter in the keyword that has been used already, you skip it.
  After the end of the keyword, the remaining letters of the alphabet are inserted, again in the order they appear.

Playfair cipher – keyword expansion

- The Playfair cipher uses a keyword.
- Encryption/decryption uses a 5×5 grid of letters.
- Turn the keyword into this grid by filling in the letters of the keyword row-wise from the top left corner.
  The grid contains each letter once, with I and J identified; so when you reach a letter in the keyword that has been used already, you skip it.
  After the end of the keyword, the remaining letters of the alphabet are inserted, again in the order they appear.
  If the keyword is SECRET then the grid looks as follows:

```
S E C R T
```

Playfair cipher – keyword expansion

- The Playfair cipher uses a keyword.
- Encryption/decryption uses a 5×5 grid of letters.
- Turn the keyword into this grid by filling in the letters of the keyword row-wise from the top left corner.
  The grid contains each letter once, with I and J identified; so when you reach a letter in the keyword that has been used already, you skip it.
  After the end of the keyword, the remaining letters of the alphabet are inserted, again in the order they appear.
  If the keyword is SECRET then the grid looks as follows:

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

  Note the skipped second E in the keyword.
  This fills up the grid completely – if you have any letters left, something went wrong earlier.

Playfair cipher – encryption

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert `X` when encountering a pair of identical letters.
  Append `X` if there is a single letter at the end.
  `HELLOBOB`

Playfair cipher – encryption

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert `X` when encountering a pair of identical letters.
  Append `X` if there is a single letter at the end.
  `HE LLOBOB`

Playfair cipher – encryption

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert `X` when encountering a pair of identical letters.
  Append `X` if there is a single letter at the end.
  `HE LX LO BO B`

Playfair cipher – encryption

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert `X` when encountering a pair of identical letters.
  Append `X` if there is a single letter at the end.
  `HE LX LO BO BX`

Playfair cipher – encryption

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

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert `X` when encountering a pair of identical letters.
  Append `X` if there is a single letter at the end.
  `HE LX LO BO BX`
- Three cases for encryption
  - If the two letters appear in the same row, encrypt each of the two letters to the letter to the right of it.
  - If the two letters appear in the same column, encrypt each of the two letters to the letter below it.
  - If the two letters span a rectangle in the grid, encrypt each of them to the letter in the same row and opposite corner.

Playfair cipher – encryption

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

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert X when encountering a pair of identical letters.
  Append X if there is a single letter at the end.
  HE LX LO BO BX
- Three cases for encryption
  - If the two letters appear in the same row, encrypt each of the two letters to the letter to the right of it.
  - If the two letters appear in the same column, encrypt each of the two letters to the letter below it.
  - If the two letters span a rectangle in the grid, encrypt each of them to the letter in the same row and opposite corner.

  HE LX LO BO BX
  IS

Playfair cipher – encryption

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

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert X when encountering a pair of identical letters.
  Append X if there is a single letter at the end.
  HE LX LO BO BX
- Three cases for encryption
  - If the two letters appear in the same row, encrypt each of the two letters to the letter to the right of it.
  - If the two letters appear in the same column, encrypt each of the two letters to the letter below it.
  - If the two letters span a rectangle in the grid, encrypt each of them to the letter in the same row and opposite corner.

  HE LX LO BO BX
  IS KY

Playfair cipher – encryption

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

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert X when encountering a pair of identical letters.
  Append X if there is a single letter at the end.
  HE LX LO BO BX
- Three cases for encryption
  - If the two letters appear in the same row, encrypt each of the two letters to the letter to the right of it.
  - If the two letters appear in the same column, encrypt each of the two letters to the letter below it.
  - If the two letters span a rectangle in the grid, encrypt each of them to the letter in the same row and opposite corner.

  HE LX LO BO BX
  IS KY IQ IW

Playfair cipher – encryption

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

- Preprocess the message: split into pairs of letters, starting from the left.
  Insert X when encountering a pair of identical letters.
  Append X if there is a single letter at the end.
  HE LX LO BO BX
- Three cases for encryption
  - If the two letters appear in the same row, encrypt each of the two letters to the letter to the right of it.
  - If the two letters appear in the same column, encrypt each of the two letters to the letter below it.
  - If the two letters span a rectangle in the grid, encrypt each of them to the letter in the same row and opposite corner.

  HE LX LO BO BX
  IS KY IQ IW DW
- To decrypt, reverse the procedure.

Hill cipher

- This system uses matrices. There is a system parameter n
- First encode the letters into numbers in $[0, 25]$.

Hill cipher

- This system uses matrices. There is a system parameter n
- First encode the letters into numbers in $[0, 25]$.
- The secret key S is an $n \times n$ matrix over $\mathbb{Z}/26$ which is invertible.
- Write let the plaintext a as vector

$$(m_1, m_2, \ldots, m_n) \in (\mathbb{Z}/26)^n.$$

- m gets encrypted into ciphertext

$$c^T = Sm^T.$$

- To decrypt compute

$$m^T = S^{-1}c^T.$$

Hill cipher

- This system uses matrices. There is a system parameter n
- First encode the letters into numbers in $[0, 25]$.
- The secret key S is an $n \times n$ matrix over $\mathbb{Z}/26$ which is invertible.
- Write let the plaintext a as vector

$$(m_1, m_2, \ldots, m_n) \in (\mathbb{Z}/26)^n.$$

- m gets encrypted into ciphertext

$$c^T = Sm^T.$$

- To decrypt compute

$$m^T = S^{-1}c^T.$$

- The inverse of S is computed in $\mathbb{Z}/26$, so you need to use the extended Euclidean algorithm (XGCD) in addition to linear algebra. For a recap of how XGCD works watch the short video.

Column transposition

3	4	7	2	5	1	6
W	R	I	T	E	T	E
X	T	I	N	F	I	X
E	D	W	I	D	T	H
R	O	W	S	T	H	E
N	P	E	R	M	U	T
E	C	O	L	U	M	N
S						

Column transposition

3	4	7	2	5	1	6
W	R	I	T	E	T	E
X	T	I	N	F	I	X
E	D	W	I	D	T	H
R	O	W	S	T	H	E
N	P	E	R	M	U	T
E	C	O	L	U	M	N
S						

1	2	3	4	5	6	7
T	T	W	R	E	E	I

Column transposition

3	4	7	2	5	1	6
W	R	I	T	E	T	E
X	T	I	N	F	I	X
E	D	W	I	D	T	H
R	O	W	S	T	H	E
N	P	E	R	M	U	T
E	C	O	L	U	M	N
S						

1	2	3	4	5	6	7
T	T	W	R	E	E	I
I	N	X	T	F	X	I

Column transposition

3	4	7	2	5	1	6
W	R	I	T	E	T	E
X	T	I	N	F	I	X
E	D	W	I	D	T	H
R	O	W	S	T	H	E
N	P	E	R	M	U	T
E	C	O	L	U	M	N
S						

1	2	3	4	5	6	7
T	T	W	R	E	E	I
I	N	X	T	F	X	I
T	I	E	D	D	H	W
H	S	R	O	T	E	W
U	R	N	P	M	T	E
M	L	E	C	U	N	O
		S				

Read out as

Column transposition

3	4	7	2	5	1	6
W	R	I	T	E	T	E
X	T	I	N	F	I	X
E	D	W	I	D	T	H
R	O	W	S	T	H	E
N	P	E	R	M	U	T
E	C	O	L	U	M	N
S						

1	2	3	4	5	6	7
T	T	W	R	E	E	I
I	N	X	T	F	X	I
T	I	E	D	D	H	W
H	S	R	O	T	E	W
U	R	N	P	M	T	E
M	L	E	C	U	N	O
		S				

Read out as

TITHUM TNISRL WXERNES RTDOPC EFDTMU EXHETN IIWWEO

Column transposition

3	4	7	2	5	1	6
W	R	I	T	E	T	E
X	T	I	N	F	I	X
E	D	W	I	D	T	H
R	O	W	S	T	H	E
N	P	E	R	M	U	T
E	C	O	L	U	M	N
S						

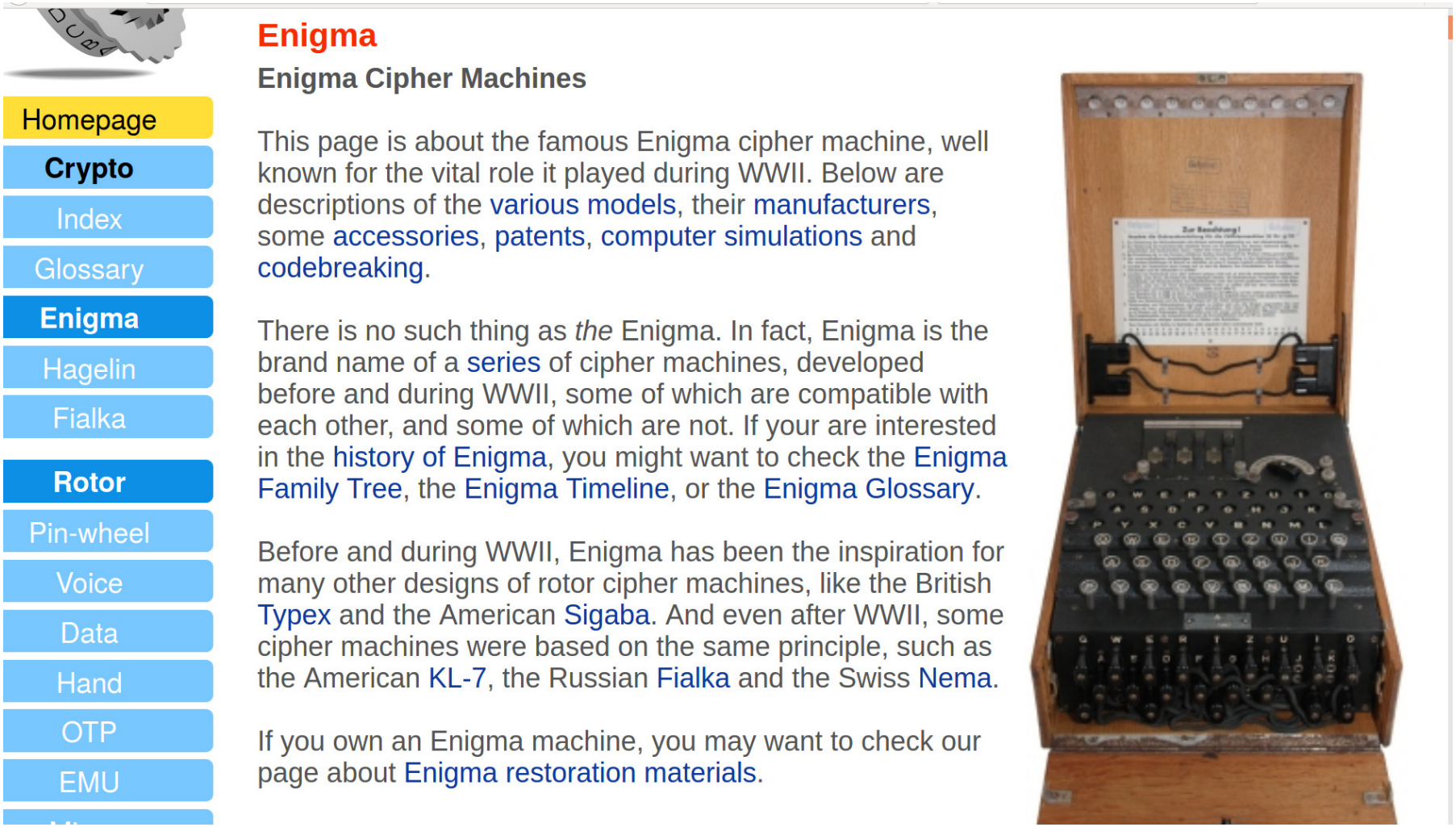
1	2	3	4	5	6	7
T	T	W	R	E	E	I
I	N	X	T	F	X	I
T	I	E	D	D	H	W
H	S	R	O	T	E	W
U	R	N	P	M	T	E
M	L	E	C	U	N	O
		S				

Read out as
TITHUMTNISRLWXERNESRTDOPCEFDTMUEXHETNIIWWEO

For this and more fun with systems you can use by hand see, e.g.,
http://rumkin.com/tools/cipher/coltrans.php

Rotor machines

Read about rotor machines in general, and the Enigma in particular, at the Crypto Museum.



They also have very informative articles about other historical ciphers.