Playfair

Substitution (bigraphisch)

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. Es werden nicht einzelne Buchstaben, sondern Buchstaben**paare** verschlüsselt. Solche Verschlüsselungen heißen **bigraphische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Bi* heißt *zwei* und *graphisch* kommt vom griechischen *graphein* = schreiben.)

Der englische Physiker Charles Wheatstone (s. Bild) erfand 1854 eine Verschlüsselung, bei der immer zwei Buchstaben auf einmal verschlüsselt werden. Sein Freund, der Politiker Lord Lyon Playfair Baron von St. Andrews, führte diese Verschlüsselung in die militärischen und diplomatischen Kreise Englands ein. Das Verschlüsselungsverfahren wurde schließlich nach jenem Politiker benannt.

Erklärung am Beispiel:

1. Sender und Empfänger einigen sich auf ein Schlüsselwort. Dieses wird in ein 5×5-Quadrat (mehrfache Buchstaben weglassen!) geschrieben. **I** und **J** werden dabei nur als ein Buchstabe gezählt. Der Rest des Alphabets wird fortlaufend dahintergeschrieben.

Beispiel

Für das Schlüsselwort **PLAYFAIR** sieht die Verschlüsselungsmatrix wie folgt aus:

p	l	a	y	f
i/j	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

2. Die Nachricht wird in Zweiergruppen aufgeschrieben. Dabei darf nie zweimal der gleiche Buchstabe in einer Gruppe stehen. Passiert das, wird ein **X** eingefügt. Steht am Ende ein Buchstabe allein, wird ein **X** angehängt.

Beispiel

Nachricht: **HALLO CHARLES** wird zu **HA LX LO CH AR LE SX**

v5 13. März 2015

3. Nun werden diese Buchstabenpaare ersetzt. Wodurch sie ersetzt werden, hängt davon ab, wo sie im Quadrat stehen:
   - Stehen beide Buchstaben in derselben Zeile, werden sie jeweils durch ihren Nachfolger in der Zeile ersetzt. (Nachfolger des letzten ist der erste Buchstabe.)
   - Stehen beide Buchstaben in derselben Spalte, werden sie jeweils durch ihren Nachfolger in der Spalte ersetzt. (Nachfolger des letzten ist der erste Buchstabe.)
   - Stehen die Buchstaben in verschiedenen Zeilen und Spalten, wird der obere der beiden durch den Buchstaben ersetzt, der in derselben Zeile wie der obere und in derselben Spalte wie der untere Buchstabe steht. Der untere wird durch den Buchstaben ersetzt, der in derselben Zeile wie der untere und in derselben Spalte wie der obere Buchstabe steht.

Beispiel

HA wird zu **QB** (gleiche Spalte)
LX wird zu **YV**:

p	l	a	y	f
i/j	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

LO wird zu **RV** (gleiche Spalte)
CH wird zu **BK**
AR wird zu **LB**
LE wird zu **PG**
SX wird zu **XY** (gleiche Spalte)

Verschlüsselte Nachricht: **QBYVRVBKLBPGXY**