BESCHREIBUNG DER PLAYFAIR CHIFFRE

Für das Playfair Verfahren brauchen wir eine Tabelle, die 5 Zeilen und 5 Spalten hat. Um so eine Tabelle mit Buchstaben zu füllen, benutzt man ein Schlüsselwort. Nehmen wir doch einfach einmal ORCHIDEE als unser Schlüsselwort.

Dann schreiben wir diese Buchstaben der Reihe nach, Zeile für Zeile in die Tabelle. Dabei lassen wir die Buchstaben weg, die wir schon in den Kasten eingetragen haben. Das E wird dann nur einmal eingetragen. Danach wird der Rest des Kastens der Reihe nach mit den Buchstaben des Alphabets gefüllt, die noch nicht im Kasten eingetragen sind. Aber wir haben doch nur 5*5=25 Einträge und 26 Buchstaben! Deswegen lassen wir das J einfach weg und machen keinen Unterschied zwischen einem I und einem J. Wenn wir zum Beispiel das Wort IUNGE entschlüsselt haben, ist ein einfach zu raten, dass dieses Wort JUNGE heißen soll. Die Tabelle für das Playfair sieht dann so aus:

O	**R**	**C**	**H**	**I**
D	**E**			

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

Wie benutzen wir jetzt so eine Playfair Tabelle? Angenommen, wir möchten einem Freund die Nachricht

ICH KOMME AM MITTWOCH schicken. Dann müssen wir diese Schritte durchführen:

1. Zuerst teilen wir den Satz wieder in Digramme auf:

   ICH KOMME AM MITTWOCH wird zu

   IC-HK-OM-ME-AM-MI-TT-WO-CH

2. Falls ein Digramm aus zwei gleichen Buchstaben besteht, fügen wir zwischen den doppelten Buchstaben ein X ein und teilen den Satz wieder in Digramme auf. Wenn am Schluss ein Buchstabe fehlt, fügen wir auch ein X ein:

ICHKOMMEAMMITTWOCH wird zu IC-HK-OM-ME-AM-MI-TX-TW-OC-HX

3. Jetzt gibt es drei verschiedene Fälle, ein Digramm mit der Playfair Tabelle zu verschlüsseln:

    a. Die zwei Buchstaben liegen in derselben Zeile der Tabelle, wie es zum Beispiel bei dem Digramm IC der Fall ist. Dann besteht das verschlüsselte Paar aus den beiden Buchstaben, die in der Tabelle rechts vom I und C liegen. Rechts vom C liegt das H, welches der Schlüsselbuchstabe für das C ist. Rechts vom I liegt kein Buchstabe, dort ist die Tabelle zu Ende. Wenn das passiert, dann nehmen wir den ersten Buchstaben in derselben Zeile als Schlüsselbuchstaben. Hier ist der Schlüsselbuchstabe für das I das O. Das verschlüsselte Digramm für IC ist also OH.

    b. Die zwei Buchstaben liegen in derselben Spalte. Das kommt in unserem Beispiel nicht vor, aber es ist zum Beispiel der Fall, wenn wir das Digramm GV verschlüsseln wollen. Dann besteht das Schlüsselpaar aus den Buchstaben, die in derselben Spalte unter dem G und dem V stehen. Unter dem G steht das P, unter dem V gibt es keinen weiteren Buchstaben. Dann nehmen wir den ersten Buchstaben in derselben Spalte, hier ist das das O. Das verschlüsselte Digramm für GV ist also PO.

    c. Die zwei Buchstaben liegen weder in derselben Zeile, noch in derselben Spalte der Tabelle. Das ist zum Beispiel der Fall bei dem Digramm HK. Um den Verschlüsselungsbuchstaben für das H zu finden, suchen wir den Eintrag, der in derselben Zeile wie H und in derselben Spalte wie K liegt. Das ist der Buchstabe R. Um den Verschlüsselungsbuchstaben für das K zu finden, suchen wir den Eintrag, der in derselben Zeile wie K und in derselben Spalte wie H liegt. Hier ist das der Buchstabe M. Das verschlüsselte Digramm für HK ist also RM.

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

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

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

Der verschlüsselte Text für IC-HK-OM-ME-AM-MI-TX-TW-OC-HX ist dann OH-RM-HG-KB-BL-NH-SY-QY-RH-CY.

Wenn unser Freund die Nachricht OHRMHGKBBLNHSYQYRHRQ erhält und sie entschlüsseln möchte, so muss er sie zuerst wieder in Digramme unterteilen: OH-RM-HG-KB-BL-NH-SY-QY-RH-CY. Er braucht dieselbe Playfair Tabelle, die wir zur Verschlüsselung benutzt haben. Es reicht aber, dass er sich das Wort ORCHIDEE gemerkt hat. Dann kann der die Tabelle einfach selbst wieder erzeugen, so wie wir es vorher auch gemacht haben. Auch für ihn gibt es drei verschiedene Fälle, wenn er ein Digramm entschlüsseln möchte:

1. Die zwei Buchstaben liegen in derselben Zeile der Tabelle, wie zum Beispiel die Buchstaben O und H. Beim Verschlüsseln haben wir die Buchstaben genommen, die rechts von ihnen standen. Also müssen unser Freund zum Entschlüsseln die Buchstaben nehmen, die links von ihnen stehen. Links vom O steht kein Buchstabe, und wie vorher auch, nimmt er dann den letzten Buchstabe der Zeile, das I. Links vom H befindet sich das C. Das entschlüsselte Digramm für OH ist also das Digramm IC.

2. Die zwei Buchstaben liegen in derselben Spalte der Tabelle. Das ist zum Beispiel der Fall bei dem Digramm PO. Zum Entschlüsseln nimmt unser Freund nicht die Buchstaben, die in derselben Zeile unter dem P und dem O liegen, sondern die, welche darüber liegen. Über dem P liegt das G und über dem O kein Buchstabe. Für das O nimmt er dann den letzten Buchstaben in derselben Spalte. Das entschlüsselte Digramm für PO ist also GV.

3. Die zwei Buchstaben liegen weder in derselben Zeile, noch in derselben Spalte. Das ist zum Beispiel bei dem Digramm RM der Fall. Hier funktioniert die Entschlüsselung genauso wie die Verschlüsselung: Unser Freund sucht den Buchstaben, der in derselben Zeile wie das R und in derselben Spalte wie das M liegt. Das ist der Buchstabe H, der die Entschlüsselung für das R ist. Um die Entschlüsselung für das M zu bestimmen, sucht er den Buchstaben, der in derselben Zeile wie das M und in derselben Spalte wie das R liegt. Dieser Buchstabe ist das K. Somit ist das entschlüsselte Digramm für RM das Digramm HK.

Ihr könnt jetzt selbst überprüfen, dass unser Freund die Nachricht OHRMHGKBBLNHSYQYRHRQ zu ICHKOMMEAMMITXTWOCHX übersetzt. Daraus kann er dann leicht die Nachricht ICH KOMME AM MITTWOCH erkennen. Jetzt müssten wir es auch schaffen, die Nachricht NPPMBKLABY zu übersetzen. Sie lautet: GUT GEMACHT.