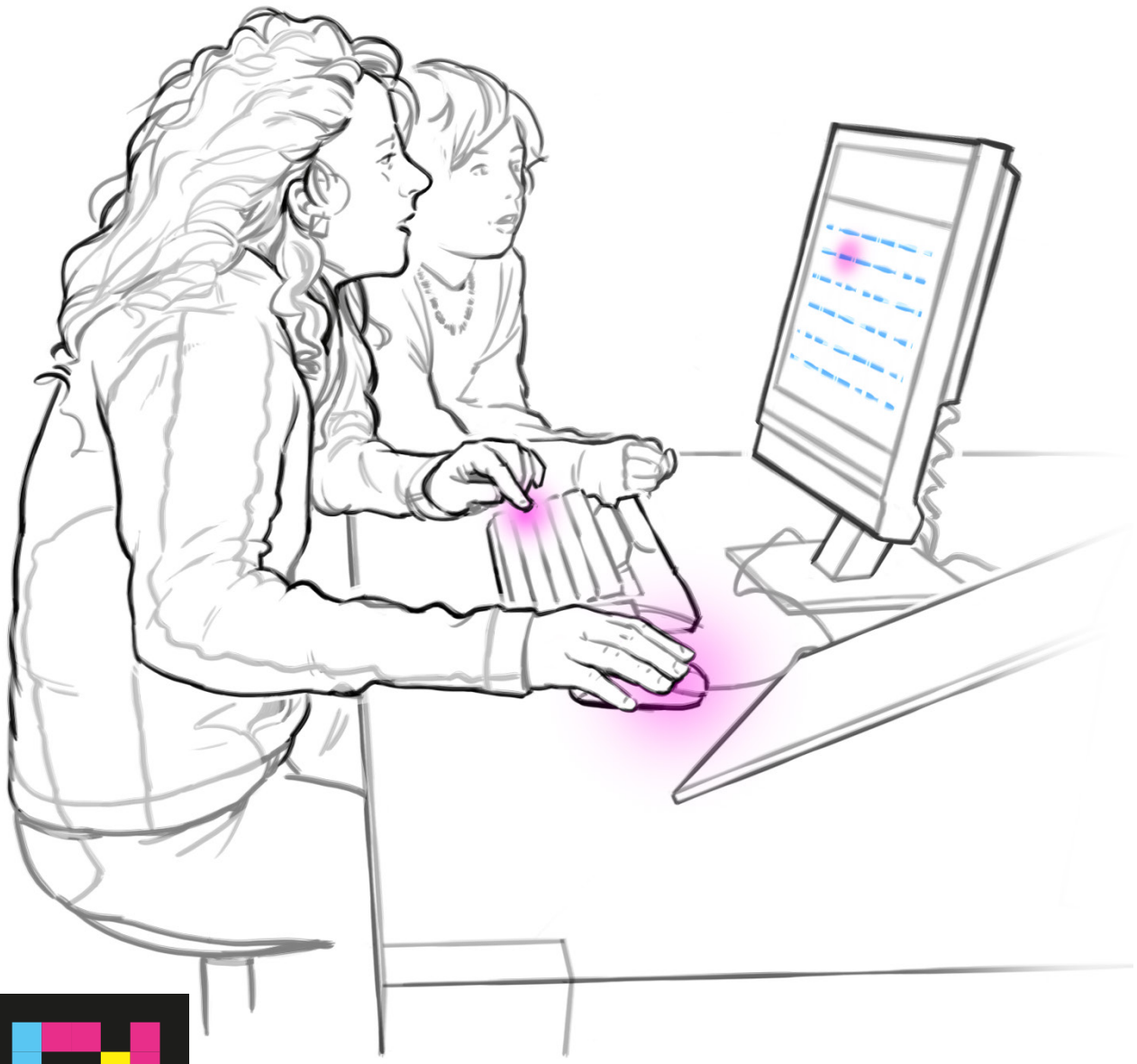
Knack den Code!

Im Entschlüsseln von Texten, die einen Sinn ergeben, sind wir Menschen wirklich gut - weil wir raten können!



Was tun und beachten:

- Man kann unter jeden Buchstaben der unverständlichen Wörter einen anderen Buchstaben setzen.
- Der Computer ersetzt jeden richtig geratenen Buchstaben sofort an jeder auftretenden Stelle. Hast Du den richtigen Buchstaben nicht erraten, bleibt das Feld weiterhin leer.
- Übrigens - bei diesem Experiment gibt es nur etwas über 400 Quadrillionen (eine Quadrillion sind eine Billion Billionen; eine Billion ist eine Million Millionen) verschiedene Verschlüsselungsmöglichkeiten - also nur Mut!
- Ein Tipp: Der verschlüsselte Text ist in deutscher Sprache verfasst.

Wer mehr wissen möchte:

lies den Zusatztext

Idee und Konzept: Thomas Kiupel (D)
Ausführung: Technoraama
“Knack den Code_DEFIL”; Nr. 10226

Knack den Code!

Im Entschlüsseln von Texten, die einen Sinn ergeben, sind wir Menschen wirklich gut - weil wir raten können!

Was tun und beachten:

- Man kann unter jeden Buchstaben der unverständlichen Wörter einen anderen Buchstaben setzen.
- Der Computer ersetzt jeden richtig geratenen Buchstaben sofort an jeder auftretenden Stelle. Hast Du den richtigen Buchstaben nicht erraten, bleibt das Feld weiterhin leer.
- Übrigens - bei diesem Experiment gibt es nur etwas über 400 Quadrillionen (eine Quadrillion sind eine Billion Billionen; eine Billion ist eine Million Millionen) verschiedene Verschlüsselungsmöglichkeiten - also nur Mut!
- Ein Tipp: Der verschlüsselte Text ist in deutscher Sprache verfasst.

Wer mehr wissen möchte:

Idee und Konzept: Thomas Kiupel (D)
Ausführung: Technoraama
“Knack den Code_DEFIL”; Nr. 10226

Knack den Code!

Wer mehr wissen möchte

«Qxpoa gvp pbuu!»

Dieses Exponat zeigt die wichtigsten Eigenschaften von Geheimcodes. In der Kryptographie spricht man von Klartexten, Geheimtexten und Schlüsseln. Der Schlüssel verrät, wie man aus dem Geheimtext den Klartext wiedergewinnen kann.

Unser Geheimtext wurde nach einem monoalphabetischen Code verschlüsselt. Das bedeutet, dass jedem Buchstaben des Klartextalphabets immer derselbe Buchstabe des Geheimtextalphabets zugeordnet wird.

Die einfachste und berühmteste Methode dieser Verschlüsselung ist die sogenannte Caesar-Verschlüsselung. Sie ist nach dem römischen Feldherrn Julius Caesar benannt, der sie zuerst benutzte. Dabei entsteht das Geheimtextalphabet dadurch, dass das normale Alphabet um eine bestimmte Anzahl von Stellen verschoben wird. Wenn um drei Stellen verschoben wird, wird ein A im Klartext ein D im Geheimtext, ein D im Klartext wird ein G usw. Dies kannst Du am benachbarten Exponat «Das Rad Caesars» ausprobieren.

Im Allgemeinen werden aber bei einem monoalphabetischen Code die Buchstaben nicht nach einem bestimmten System, etwa einer Verschiebung, ersetzt, sondern «kreuz und quer». Das heisst, jede Permutation der Buchstaben ist eine mono-alphabetische Verschlüsselung.

Ein Beispiel: Jedes A des Klartextalphabets wird zu einem X des Geheimtextes, jedes B wird zu einem W, jedes C zu einem Z usw.

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

In diesem Beispiel würde der Klartext «Mathe ist toll» zu dem Geheimtext «Qxpoa gvp pbuu». Der Schlüssel ist in diesem Fall die eindeutige Zuordnung eines Geheimtextbuchstabens zu einem Klartextbuchstaben. Man kann sich die Anzahl der Möglichkeiten für verschiedene Schlüssel kaum vorstellen. Es gibt genau

26! = 26x25x24x23x....x3x2x1= 403’291’461’126’605’635’584’000’000

verschiedene Schlüssel (d.h. über 400 Quadrillionen; eine Quadrillion ist eine Billion Billionen – eine Billion ist eine Million Millionen!). Der Computer wählt sich zufällig einen Schlüssel aus.

Wie kann man nun den Geheimtext entschlüsseln, ohne den Schlüssel zu kennen? Dabei hilft eine einfache Strategie: Man sucht zunächst nach kurzen, häufig auftretenden Wörtern des Geheimtextes und versucht, diese zu entschlüsseln. Zum Beispiel können die dreibuchstabigen Wörter im Geheimtext «und», «ein», «der», «die», «das», «sie», «ich» usw. heissen. Eine andere Taktik ist, den häufigsten Buchstaben des Geheimtextes zu suchen und diesen dann durch „E“, den häufigsten Buchstaben der deutschen Sprache, zu ersetzen.

Das Experiment zeigt, dass man mit etwas Köpfchen den Code knacken kann, obwohl es eine riesige Zahl von Schlüsseln gibt.

Literatur

(1) Beutelspacher, A.: Kryptologie. Verlag Vieweg, Wiesbaden, 6. Auflage 2001.

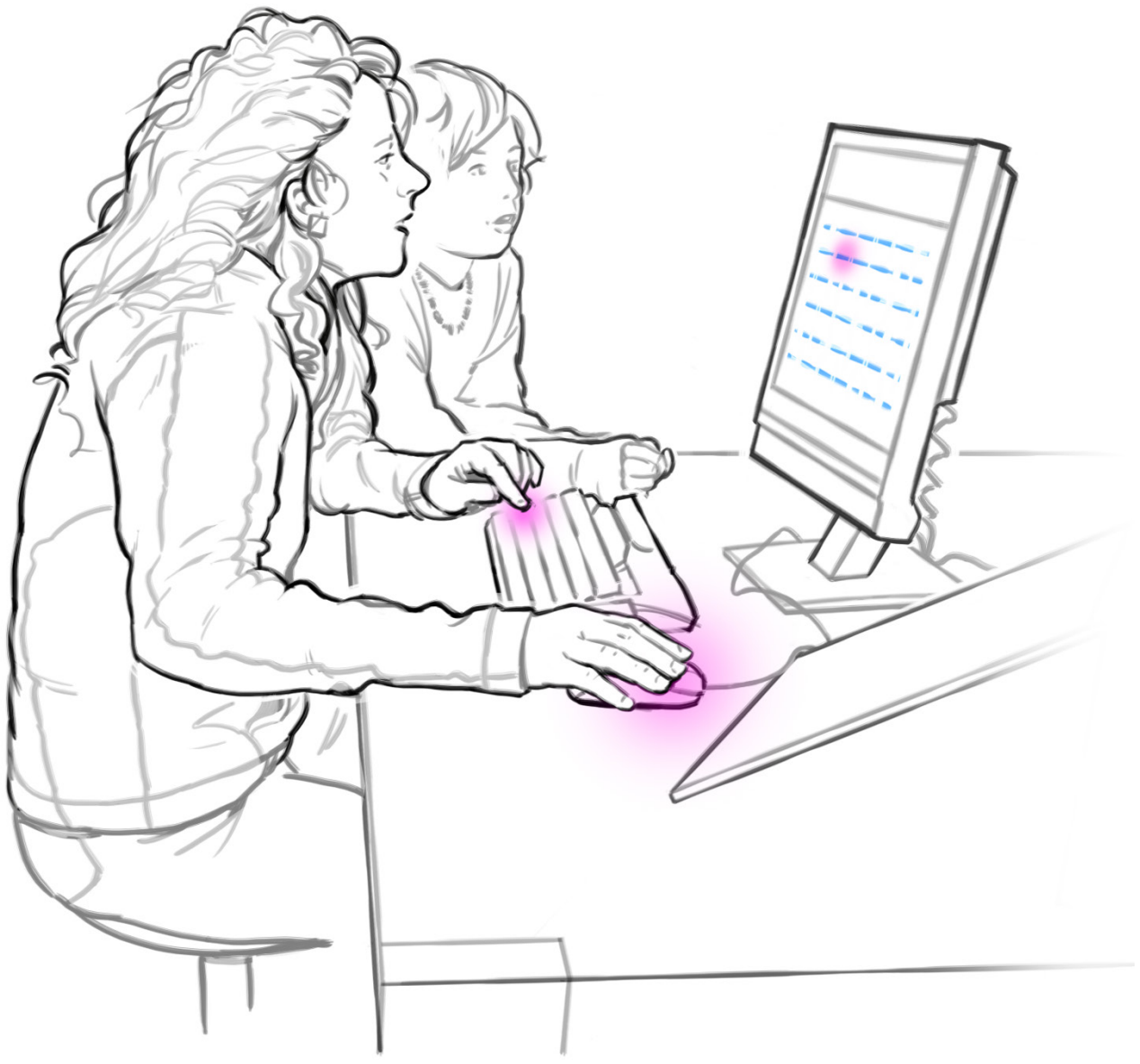
(2) Beutelspacher, A.: Geheimsprachen. Gschichte und Techniken. C.H.Beck, München, 3. Auflage 2002.

Was tun und beachten:

Idee und Konzept: Thomas Kiupel (D) / Ausführung: Technoraama
“Knack den Code_DEFIL”; Nr. 10226

Crack the Code!

We humans are really good at cracking coded messages – because we can guess!



To do and notice:

- Choose a substitute letter to put under any letter in the coded message.
- If you have guessed right, the computer will fill this letter in wherever it occurs. If wrong, nothing happens!
- By the way, there are over 40 quadrillion possible ways of replacing the alphabet with alternative letters (26 x 25 x 24 x etc = 4.032×10^{26}). Don't be deterred!
- Tip:
  The coded text is in German!

Want to know more?

Idea and ConCept: Thomas Kiupel (D)
Realisation: Technoraama
"Knack den Code_DEFIL"; Nr. 10226

Crack the Code!

Want to know more?

«Qxpoa gvp pbuu!»

This exhibit illustrates the most important aspects of secret codes. In cryptography one speaks of plain text, cipher text and the key – using the key decodes cipher text into the plain text, which you can then understand.

Our code here is monoalphabetic, the simplest sort, where each letter is replaced by a different one, but always the same. Julius Caesar (1st century AD) used the simplest form of this code for military messages, where each letter was replaced by the letter a fixed number of places along the alphabet.

For example, if the number of places was 3, then A in the plain text would be replaced by D in the cipher text, D by G, etc. This three-place shift was actually used by Caesar (according to his biographer, Suetonius (2nd century AD), and is called Caesar's cipher.

Fixed shift codes are too simple for security, and a non-systematic substitution, as below, is more difficult to crack.

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

In this example, plain text «maths is cool» converts to cipher text «qxpoa gvp pbuu»!

The number of possible simple substitution keys is astronomical:

26! = 26x25x24x23x....x3x2x1= 403'291'461'126'605'635'584'000'000 approximately.

Even for a huge computer, it would be stupid to attempt to try these out one by one without a strategy.

A useful way of hitting on the right key is to look at the short words which recur: e.g. the, one, and, for, etc. Another is more statistical: knowing the frequency at which particular letters, repeated letters, etc generally occur in the language, might give clues to some words. In this way, one can vastly reduce the number of possible keys and begin to crack the code.

The Enigma machine, used by the German forces during WW2, used a substitution alphabet which changed after each letter in the plain text, and presented a formidable challenge to the code breakers!

Literature

(1) Beutelspacher, A.: Kryptologie. Verlag Vieweg, Wiesbaden, 6. Auflage 2001.

(2) Beutelspacher, A.: Geheimsprachen. Geschichte und Techniken. C.H.Beck, München, 3. Auflage 2002.

To do and notice:

Idea and ConCept: Thomas Kiupel (D)
Realisation: Technoraama
"Knack den Code_DEFIL"; Nr. 10226

Cassez le code!

Les humains sont très doués pour déchiffrer des textes qui ont un sens – parce que nous savons très bien deviner... !

A vous de jouer:

- On peut placer une autre lettre sous les lettres des mots in-com-préhensibles.
- L'ordinateur remplace immédiatement chaque lettre que vous avez devinée correctement, à chaque emplacement où elle apparaît. En revanche, le champ restera vide comme avant si vous n'avez pas deviné la lettre correcte.
- D'ailleurs – dans cette expérience il n'y a que 400 quadrillions (un quadrillion est un billion de billion, un billion est un million de million) de possibilités de déchiffrage – courage!
- Un indice: le texte codé est rédigé en allemand.

Pour en savoir plus:

Idee und Konzept: Thomas Kiupel (D)
Ausführung: Technoraama
"Knack den Code_DEFIL"; Nr. 10226

Cassez le code!

Pour en savoir plus

«Qxpoa gvp pbuu!»

Cette expérience vous montre les propriétés les plus importantes d'un code secret. En cryptographie on parle de textes en clair, de textes secrets et de clés de déchiffrement. La clé nous dit comment on peut reconstituer le texte en clair à partir du texte secret. Cela signifie que chaque lettre du texte en clair est toujours codée par la même lettre du texte secret.

La méthode la plus simple et la plus connue de ce codage est le «chiffre de César». Elle a été appelée d'après le commandant romain Jules César qui l'a utilisé en premier. L'alphabet secret est créé en déplaçant l'alphabet normal d'un certain nombre de chiffres. Quand on le déplace de 3 chiffres, un A du texte en clair devient un D du texte secret, un D du texte en clair devient un G etc. Vous pouvez tester cela dans la manip' «La roue de César».

Mais en général, dans un code monoalphabétique les lettres ne sont pas remplacées selon un certain système, comme un décalage, mais «dans tous les sens». Cela veut dire que chaque permutation des lettres est un codage monoalphabétique.

Un exemple: Chaque A du texte en clair devient un X du texte secret, chaque B devient un W, chaque C devient un Z et ainsi de suite.

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

Dans notre exemple la phrase «Mathe ist toll» («Les maths sont supers!») deviendrait «Qxpoa gvp pbuu» dans le texte secret.

Dans ce cas, la clé une règle précise qui dit comment chaque lettre du texte secret est associée à une lettre du texte clair.

On peut difficilement imaginer le nombre de possibilités de clés différentes ! Il y a exactement

26! = 26x25x24x23x....x3x2x1= 403'291'461'126'605'635'584'000'000

clés différentes (c'est-à-dire plus de 400 quadrillions, un quadrillion est un billion de billion, un billion est un million de million!). L'ordinateur choisit une clé au hasard.

Comment est-ce qu'on peut déchiffrer le texte secret sans connaître la clé? On peut se servir d'une stratégie simple: On cherche d'abord des mots courts qui reviennent souvent dans le texte secret et on essaie de déchiffrer ceux-là. Par exemple, les mots à 3 lettres dans le texte secret pourraient être «und», «ein», «der», «die», «das», «sie», «ich» etc. (en allemand). Une autre stratégie est de chercher la lettre la plus fréquente du texte secret et de la remplacer par «E», la lettre la plus fréquente dans la langue allemande.

Cette expérience montre qu'on peut casser le code en réfléchissant un peu, même s'il existe un nombre gigantesque de clés.

Littérature

(1) Beutelspacher, A.: Kryptologie. Verlag Vieweg, Wiesbaden, 6. Auflage 2001.

(2) Beutelspacher, A.: Geheimsprachen. Geschichte und Techniken. C.H.Beck, München, 3. Auflage 2002.

A vous de jouer:

Idee und Konzept: Thomas Kiupel (D)
Ausführung: Technoraama
"Knack den Code_DEFIL"; Nr. 10226

Decifra il codice segreto!

Quando si tratta di decifrare testi che hanno un senso, noi esseri umani siamo veramente bravi, perché siamo capaci di indovinare!

Che cosa fare:

- Ogni lettera delle parole incomprensibili può essere sostituita da un‘altra lettera.
- Il computer sostituisce automaticamente ogni lettera indovinata correttamente in tutti i luoghi in cui essa compare. Se invece non avete indovinato la lettera giusta, il campo continua a rimanere vuoto.
- Comunque in questo esperimento ci sono solo 400 quadrilioni (bilioni di bilioni) di possibilità diverse: forza e coraggio dunque!
- Attenzione: il testo cifrato dal computer è in tedesco.

Vuole saperne di più?

Ideazione e progetto: Thomas Kiupel (D)
Realizzazione: Technoraama
“Knack den Code_DEFIL”; Nr. 10226

Decifra il codice segreto!

Vuole saperne di più?

«Ux qxpaqxpgzx a wauux!»

Questo esperimento vi presenta le proprietà più importanti dei codici segreti. In crittografia si parla di testi in chiaro, di testi cifrati e di chiavi. La chiave permette di recuperare il testo in chiaro dal testo cifrato.

Il nostro testo è stato cifrato in base a un codice monoalfabetico. Questo significa che a ogni lettera dell'alfabeto in chiaro corrisponde sempre la stessa lettera dell'alfabeto cifrato.

Il metodo più semplice e famoso per effettuare questa operazione di codifica è il cosidddetto codice Cesare. Esso prende il nome da quello del famoso generale romano Giulio Cesare, che fu il primo a impiegarlo. L'alfabeto cifrato viene ottenuto trasponendo l'alfabeto originario di un certo numero di posti. Se questo numero è di tre lettere, allora una A in chiaro viene codificata come D nel testo cifrato e una D in chiaro viene codificata come G ecc. Potete sperimentare questo sistema nell'esperimento qui vicino intitolato «La ruota di Cesare».

In generale, le lettere in un codice monoalfabetico non vengono sostituite in base a un determinato sistema, per esempio con una semplice trasposizione, bensì incrociando e scambiando. Questo significa che ogni permutazione delle lettere è una codifica monoalfabetica.

Un esempio: Ogni A dell'alfabeto in chiaro viene trasformata in una X del testo segreto, ogni B diventa una W, ogni C diventa una Z ecc.

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

Nell'esempio riportato sopra, il testo in chiaro «La matematica è bella» è stato cifrato ottenendo «Ux qxpaqxpgzx a wauux». La chiave in questo caso consiste nella corrispondenza univoca di una lettera del testo cifrato a una lettera del testo in chiaro. Il numero di possibilità per le diverse chiavi è quasi inimmaginabile. Esistono esattamente

26! = 26x25x24x23x....x3x2x1= 403'291'461'126'605'635'584'000'000

diverse chiavi cioè oltre 400 quadrilioni (un quadrilione è un bilione di bilioni, mentre un bilione è un milione di milioni)! Il computer sceglie una chiave a caso.

Come è possibile decrittare un testo cifrato senza conoscere la chiave del codice? Per farlo, basta una semplice strategia. Si cercano anzitutto brevi parole, che compaiono frequentemente nel testo cifrato e si cerca di decrittare queste. Per esempio le parole di tre lettere nel testo cifrato potrebbero essere «uno», «una», «per», «con», «del», «gli» ecc. Un'altra tattica consiste nel cercare le lettere più frequenti del testo e sostituirle con la lettera A, la lettera più comune dell'alfabeto italiano (in quello tedesco sarebbe la E).

Questo esperimento dimostra che con un po' di ingegno è possibile decrittare il codice, anche quando il numero di chiavi possibili è enorme.

Bibliografia

(1) Ferragina Paolo, Luccio Fabrizio, Crittografia. Principi, algoritmi, applicazioni, Bollati Boringhieri, Torino 2001.

(2) Leonesi Stefano e Toffalori Carlo, Numeri e crittografia, Springer Verlag, Milano 2006.

Che cosa fare:

Ideazione e progetto: Thomas Kiupel (D)
Realizzazione: Technoraama
"Knack den Code_DEFIL"; Nr. 10226

Knack den Code!

Leichte Sprache

Was steht im Computer?
Du kannst es heraus·finden.

Probiere aus:
Welcher Buch·stabe heisst wie?

Was tun:

Schreibe unter den ersten Buch·staben
einen anderen Buch·staben.

Der Buch·stabe ist richtig?
Der Buch·stabe bleibt auf dem Bild·schirm.
Und:
Bei allen gleichen Buch·staben
kommt der richtige Buch·stabe auch.
Gehe zum nächsten Buch·staben.

Der Buch·stabe ist falsch?
Der Buch·stabe verschwindet wieder.

Probiere es
mit einem anderen Buch·staben.
Das Rätsel ist sehr schwierig.
Du kannst es vielleicht **nicht** lösen.
Das geht vielen Leuten so.

Mehr Informationen:

Idee und Konzept: Thomas Kiupel (D)
Ausführung: Technoraama
“Knack den Code_DEFIL”; Nr. 10226

Leichte Sprache

Knack den Code!

Mehr Informationen:

Der Text im Computer ist ver·schlüsselt.
Ver·schlüsselt heisst:
Du kannst den Text nicht lesen.
Du musst zuerst heraus·finden:
Welcher Buch·staben heisst was?
Zum Beispiel:
H heisst D
A heisst F
L heisst M
O heisst I

DFMMI heisst
HALLO

Du willst den Text lesen?
Dann musst Du den Text ent·schlüsseln.
Das heisst:
Du musst herausfinden:
Welcher Buch·stabe heisst was?
Meistens machen wir das so:
Wir raten.

Es gibt ein Trick:
Ich schaue:
Wo hat es ein Wort mit 3 Buch·staben?
Das könnte heissen:
Und
Ein
Der
Die
Das

Ich probiere aus:
Beginnt das Wort mit u?
Oder mit e?
Oder mit d?

So mache ich weiter.

Oder:
Ich kann auch schauen:
Welcher Buch·stabe kommt ganz oft?
Dann schreibe ich dort «e».
«E» kommt am häufigsten vor in Deutsch.

Was tun:

Idee und Konzept: Thomas Kiupel (D) / Ausführung: Technoraama
“Knack den Code_DEFIL”; Nr. 10226