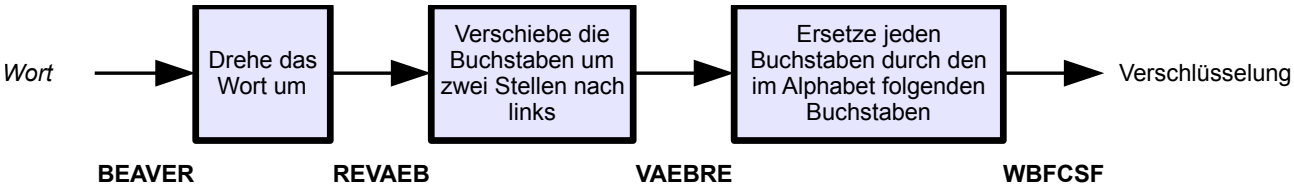
Welches Wort?

Alex und Betty senden sich verschlüsselte Nachrichten.

Dabei verschlüsseln sie jedes Wort einzeln, und zwar in drei Schritten nach folgender Vorschrift:



Das Wort BEAVER (engl. für Biber) wird somit zu WBFCSF.

Betty empfängt diese Verschlüsselung von Alex: PMGEP. Welches Wort hat Alex verschlüsselt?

A) LODGE

B) RIVER

C) FLOOD

D) KNOCK

Lösung:

Antwort C ist richtig: FLOOD

Aus der Verschlüsselung kann das ursprüngliche Wort berechnet werden, indem die Schritte der Verschlüsselungsvorschrift einzeln und in umgekehrter Reihenfolge rückgängig gemacht werden:

1. Ersetze jeden Buchstaben durch den im Alphabet vorangehenden Buchstaben.
2. Verschiebe die Buchstaben um 2 Stellen nach rechts.
3. Drehe das Wort um.

Wir wenden diese Entschlüsselungsschritte auf „PMGEP“ an:

PMGEP → OLFDO → DOOLF → FLOOD

Das Ergebnis ist eindeutig, also sind die anderen Antworten falsch.

Es ist aber in diesem Fall auch möglich, auf direkterem Weg die richtige Antwort zu bestimmen: PMGEP ist u.a. durch eine Verschiebung von Buchstaben entstanden. Im ursprünglichen Wort müssen also zwei gleiche Buchstaben aufeinander folgen. Das ist nur bei FLOOD der Fall.

Das ist Informatik!

Alex und Betty versuchen, ihre Nachrichten durch Verschlüsselung geheim zu halten. Damit beschäftigen sich Menschen bereits seit Jahrtausenden. Aus dem Verschlüsseln von Information (*Kryptographie*) und der Gewinnung von Information aus verschlüsselten Daten (*Kryptoanalyse*) ist eine ganze Wissenschaft geworden, die Kryptologie. Die Methode, die Alex und Betty verwenden, enthält Schritte, die auch in bekannten Verfahren der Kryptologie vorkommen: Bei den ersten beiden Schritten handelt es sich jeweils um eine *Transposition*, also einer Umsortierung der Zeichen einer Nachricht. Beim dritten Schritt handelt es sich um eine *Substitution*, bei der Zeichen durch andere ersetzt werden.

Trotz dieser Kombination ist die in dieser Aufgabe beschriebene Methode keinesfalls sicher. Sie wird nicht durch unterschiedliche Schlüssel variiert, und mit Hilfe statistischer Analysen lässt sich dieser Code leicht knacken – insbesondere dann, wenn man bei der Kryptoanalyse einen Computer einsetzt, der beliebig viele Entschlüsselungsversuche unternehmen kann, ohne jemals die Konzentration und die Lust zu verlieren.