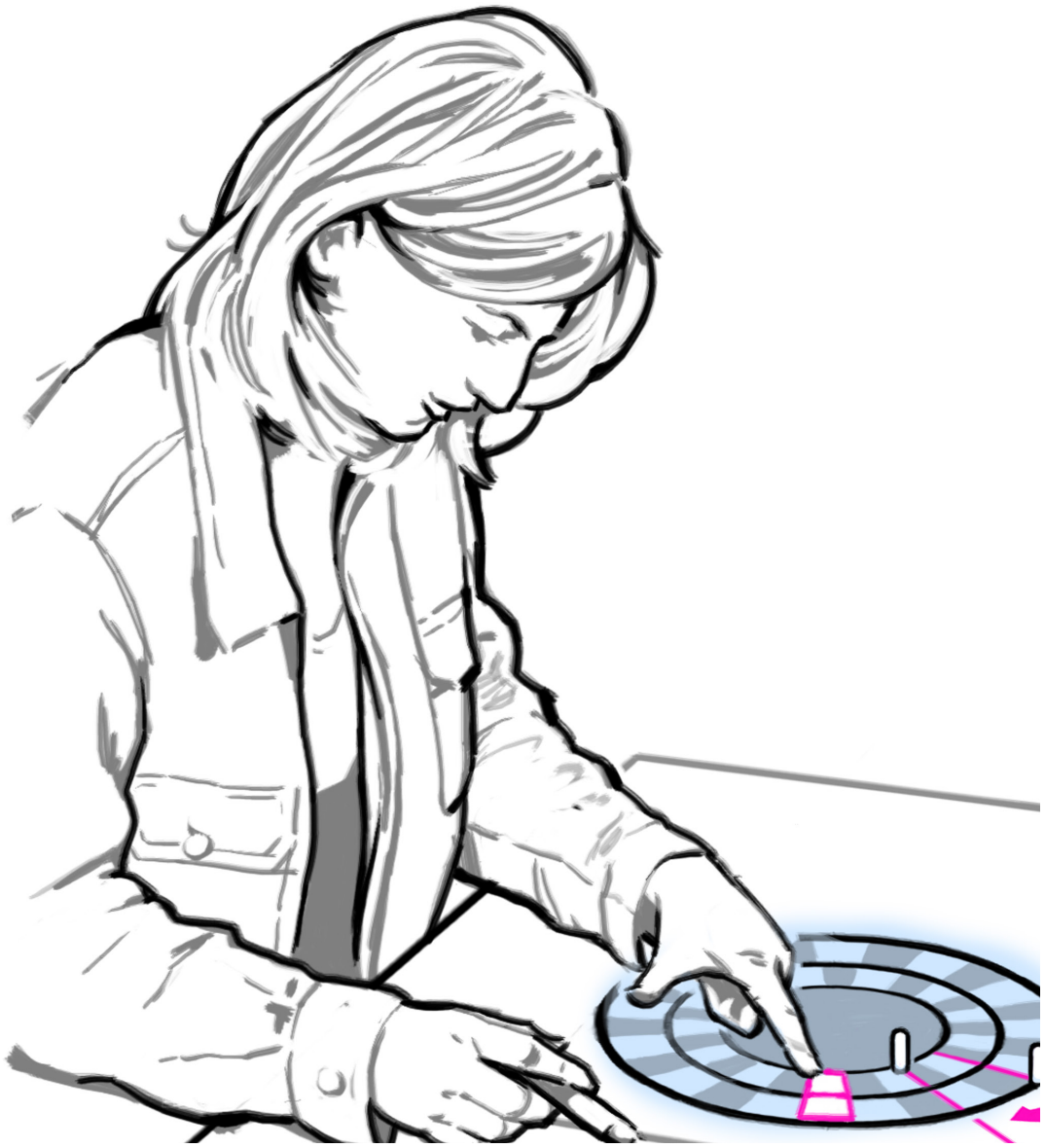
Text verschlüsseln

Das Rad Caesars

Mit solchen Methoden wurden schon zu Caesars Zeiten Informationen geschützt - allerdings oft auch zu schnell wieder entschlüsselt.



Was tun und beachten:

- *Die beiden Ringe lassen sich gegeneinander verdrehen, so dass jedem Buchstaben ein neuer Buchstabe zugeordnet wird. Stellen Sie eine beliebige Stellung ein:*
- *Schreiben Sie einen kurzen Text (in Grossbuchstaben).*
- *Suchen Sie jeden Buchstaben des Originaltextes (= Klartext) auf dem äusseren Ring und notieren Sie den entsprechenden Buchstaben des innern Ringes. So entsteht ein verschlüsselter Text (= Geheimtext).*
- *Beim Entschlüsseln gehen Sie genau umgekehrt vor, müssen dabei aber zunächst erst die Stellung der Ringe herausfinden!*
- *Fordern Sie einen Partner auf, einen von Ihnen codierten Text zu entziffern.*

Wer mehr wissen möchte:

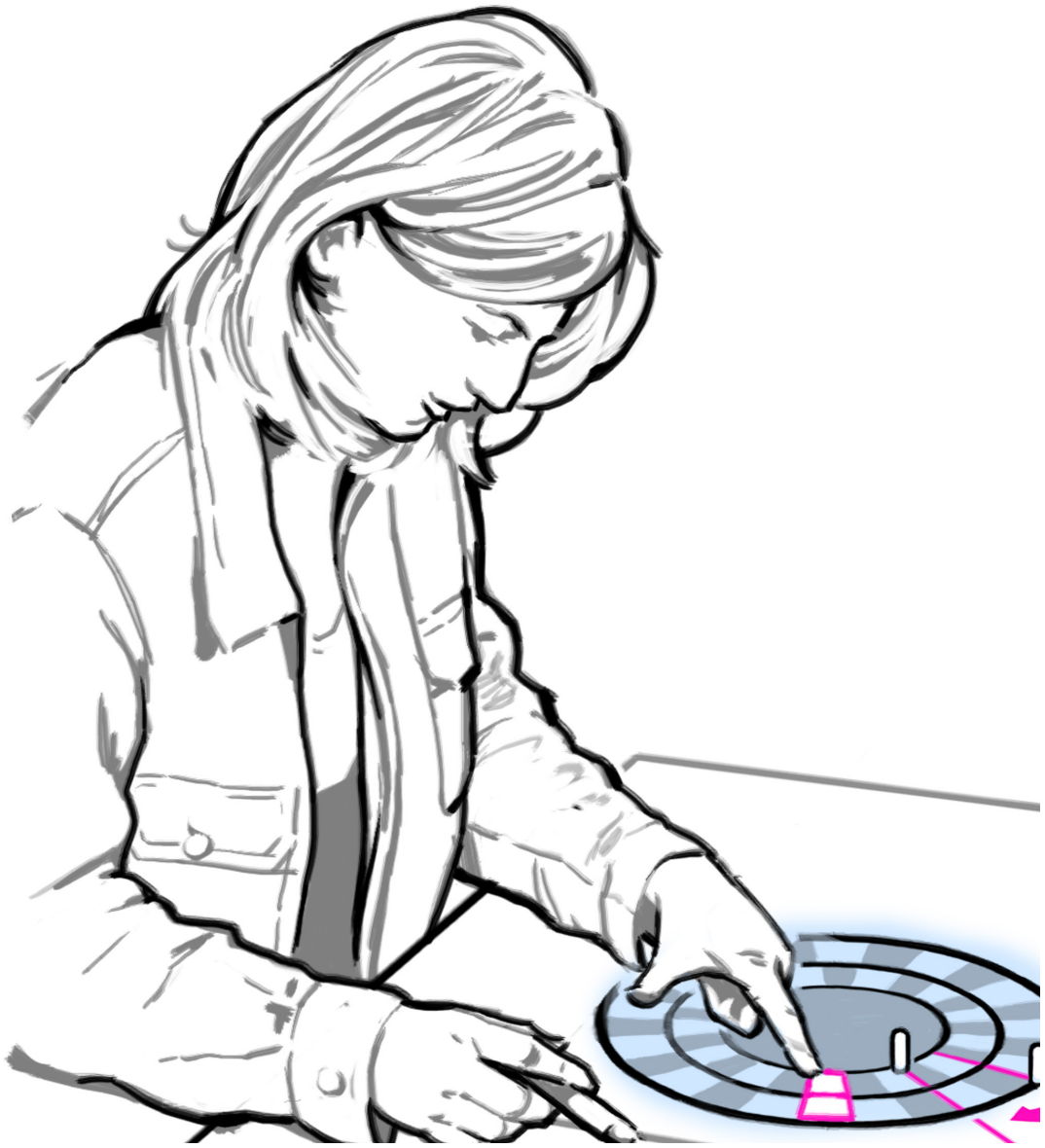
lesen Sie den Zusatztext

Idee und Konzept: Mathematikum Giessen (D)
“Text verschlüsseln_DEFI.indd”; Nr. 10440

Text verschlüsseln

Das Rad Caesars

Mit solchen Methoden wurden schon zu Caesars Zeiten Informationen geschützt - allerdings oft auch zu schnell wieder entschlüsselt.



Was tun und beachten:

- *Die beiden Ringe lassen sich gegeneinander verdrehen, so dass jedem Buchstaben ein neuer Buchstabe zugeordnet wird. Stellen Sie eine beliebige Stellung ein:*
- *Schreiben Sie einen kurzen Text (in Grossbuchstaben).*
- *Suchen Sie jeden Buchstaben des Originaltextes (= Klartext) auf dem äusseren Ring und notieren Sie den entsprechenden Buchstaben des innern Ringes. So entsteht ein verschlüsselter Text (= Geheimtext).*
- *Beim Entschlüsseln gehen Sie genau umgekehrt vor, müssen dabei aber zunächst erst die Stellung der Ringe herausfinden!*
- *Fordern Sie einen Partner auf, einen von Ihnen codierten Text zu entziffern.*

Wer mehr wissen möchte:

Idee und Konzept: Mathematikum Giessen (D)
“Text verschlüsseln_DEFI.indd”; Nr. 10440

Text verschlüsseln

Das Rad Caesars

Wer mehr wissen möchte

Die sogenannte Caesar-Verschiebung als Verschlüsselungstechnik ist wohl die simpelste Variante einer «monographisch» monoalphabetischen Substitution. Das heisst, dass jeder einzelne Buchstabe einer Nachricht (Klartext) durch einen anderen Buchstaben ersetzt wird (substituiert), indem er um eine bestimmte Anzahl Positionen im Alphabet verschoben wird. Bei einer Verschiebung um vier Positionen wird aus «A» ein «E» - man würde dies als «Schlüssel D» bezeichnen (D: vierter Buchstabe).

Diese Art der Verschlüsselung ist für den praktischen Einsatz nicht geeignet, weil das Knacken des Code sehr leicht möglich ist.

In jeder Sprache werden einzelne Buchstaben unterschiedlich häufig verwendet. Bestimmte Worte sind aufgrund Ihrer Länge auch schnell zu identifizieren (z.B. häufige Worte mit drei Buchstaben: und, vor, ich, ...) Man nehme also ein häufiges Wort wie «und». Dann schreibe man alle möglichen Verschlüsselungen auf: UND --> VOE --> WPF --> ... (Versatz der beiden Alphabete um 1,2,3 .. Buchstaben). Nach spätestens 25 Versuchen hat man den Schlüssel gefunden, da man eine dieser Kombinationen im „Geheimtext“ findet. Die Schlüssellänge, ein heute ja oft genutztes Wort, beträgt daher nur 5 bit.

Die Verschlüsselung kann sehr viel sicherer gemacht werden, wenn man erstens den vollständigen Zeichensatz (mit Kleinbuchstaben und Sonderzeichen) benützt und zudem nach einer Anzahl Buchstaben die Verschiebung ändert. Beispiel: Immer nach vier Buchstaben dreht man eine der Scheiben um so viele Positionen weiter, wie die Ziffernfolge in der Zahl π angibt 3 1 4 1 5 9 2 6 .....

Moderne Verschlüsselungsverfahren nutzen deutlich längere Schlüssel. Die heute für sicher gehaltene Verschlüsselung nach AES basiert auf mindestes 128 - 256 bit langen Schlüsseln. Solche Techniken werden im Wireless LAN (Funknetzwerke im Computerbereich) oder auch in der Computertelefonie verwendet.

Übrigens handelt es sich hierbei um eine symmetrische Verschlüsselung - der gleiche Schlüssel wird zum Ver- und Entschlüsseln genutzt. Das bedeutet aber auch, dass Sender und Empfänger den Schlüssel kennen und geheim halten müssen.

Emailverschlüsselung oder die Sicherheit im Internet (https://....) basieren demgegenüber auf asymmetrischen Verschlüsselungen, die mit privaten und öffentlichen Schlüsseln arbeiten. Der öffentliche Schlüssel wird, wie der Name sagt, öffentlich gemacht. Jeder andere Anwender kann diesen Schlüssel verwenden, um Nachrichten an den Eigentümer des Schlüssels zu verschlüsseln.

Der private Schlüssel dagegen wird vom Besitzer geheim gehalten. Er dient dazu, an ihn gesendete, mit dem öffentlichen Schlüssel verschlüsselte Nachrichten (Geheimtexte) wieder zu entschlüsseln.

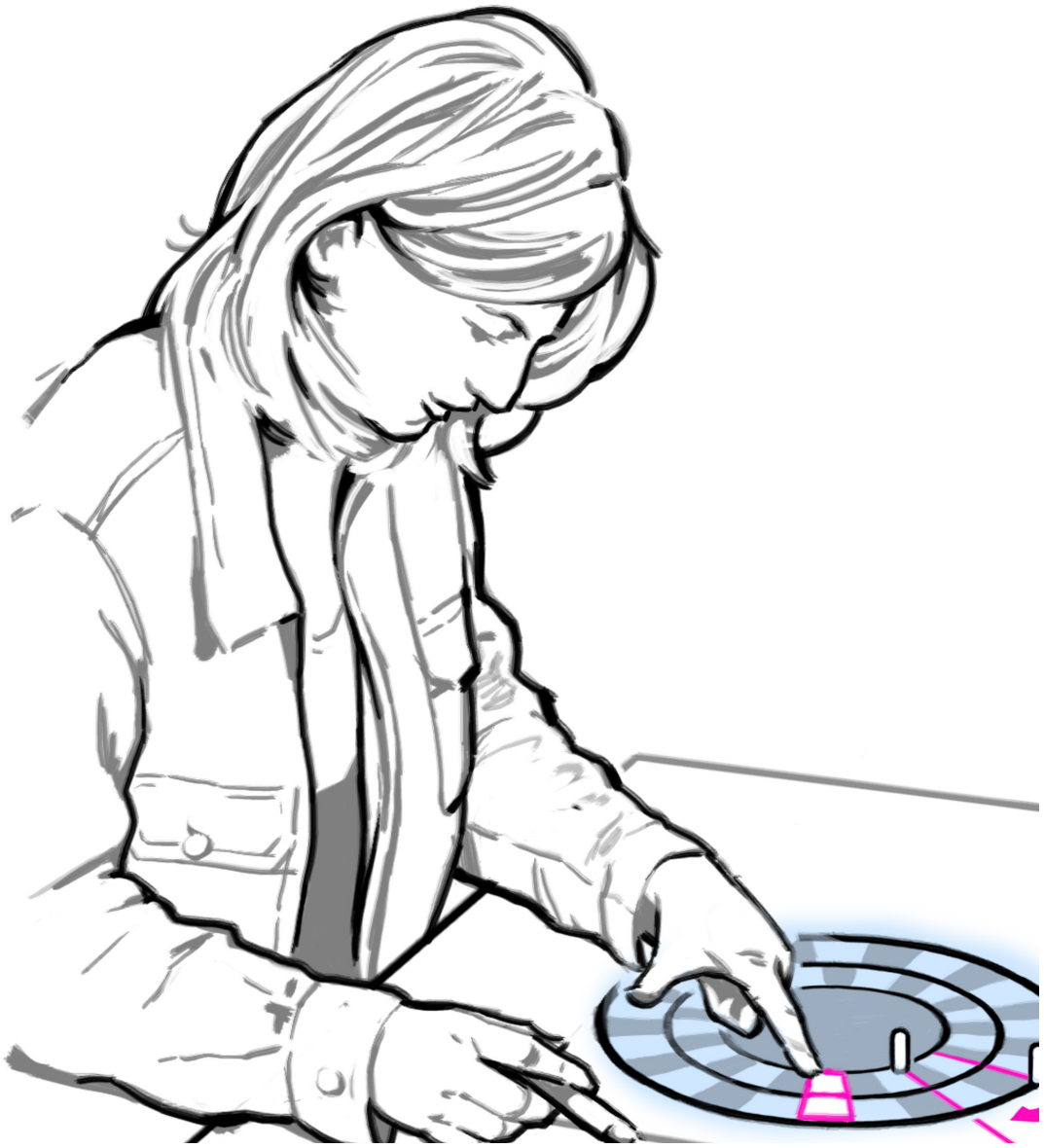
Was tun und beachten:

Idee und Konzept: Mathematikum Giessen (D)
“Text verschlüsseln_DEFI.indd”; Nr. 10440

Encoding Text

Caesar's disc

Even in ancient Rome codes like this were used to protect information – they could, however, easily be cracked.



To do and notice:

- *The rings of letters can be adjusted, so that every letter can be moved next to a different one. Choose a setting:*
- *Write a short message (in Capitals).*
- *Locate each letter of the original text (plaintext) on the outer ring, and note the corresponding letter on the inner ring. Now you can encode (encrypt) your message into "ciphertext".*
- *To decode (decrypt) a message, you reverse the procedure – but first you need to find out the setting of the rings!*
- *Ask a partner to crack your code (decipher your message)!*

Want to know more?

Idea and Concept: Mathematikum Giessen (D)
"Text verschlüsseln_DEFI.indd"; Nr. 10440

Encoding Text

Caesar's disc

Want to know more?

Caesar's method of encoding messages is easily the simplest type encrypting a message by single letter substitution. Each letter of the message (plaintext) is replaced by the letter which is a fixed number of places away along the alphabet. For example, with a shift of four places, an "A" is replaced by an "E", and this would be called "key-D substitution", because D is the fourth letter of the alphabet.

This kind of code is not suitable for practical purposes, as it is far too easy to break.

In any language, different letters are used with different frequency, as are particular words. Words may also be quickly identified if they are short (e.g. words with three letters – the, and, you, …). Taking the word "THE", you can write down all of the possible encryptions; THE --> UIF, --> VJG, --> WKH, ….(replacing letters by 1, 2, 3, etc shifts along the alphabet). Searching the encrypted message will very soon (in no more than 25 shifts) reveal the key which is being used. It is worth noting here that the "key" length in this simple system is only 5 bits (in computerspeak).

The system can be made more secure by first starting from the full letter set – lower and upper case, plus comma, full stop, etc., and arranging to change the key (the number of letters shifted along the alphabet) at intervals along the message. For example: After every four characters (letters plus punctuation marks), the key is shifted further along the alphabet by the number of places given in the number π: 3 1 4 1 5 9 2 6 .....

Modern encryption methods use considerably longer keys. The Advanced Encryption Standard (AES), adopted by the US government, encrypts plaintext in blocks of 128 bits (computerspeak) with long keys (128 bits or more) and several rounds of transformation to achieve the final ciphertext, all to produce secure transmission of sensitive messages via computer networks.

So far we have described "symmetric" systems, where the sender and receiver of the message use the same key, which must therefore be shared, but kept secret from any potential "code breaker".

Since the mid-1970s, there have been "asymmetric" systems developed, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys, a public key and a private key. Each private key is kept secret, whilst the public key is known to both sender and recipient. Messages are encrypted with the recipient's public key but can only be decrypted with the corresponding private key. The keys are related mathematically, but the private key cannot be feasibly be derived from the public key by any outsider.

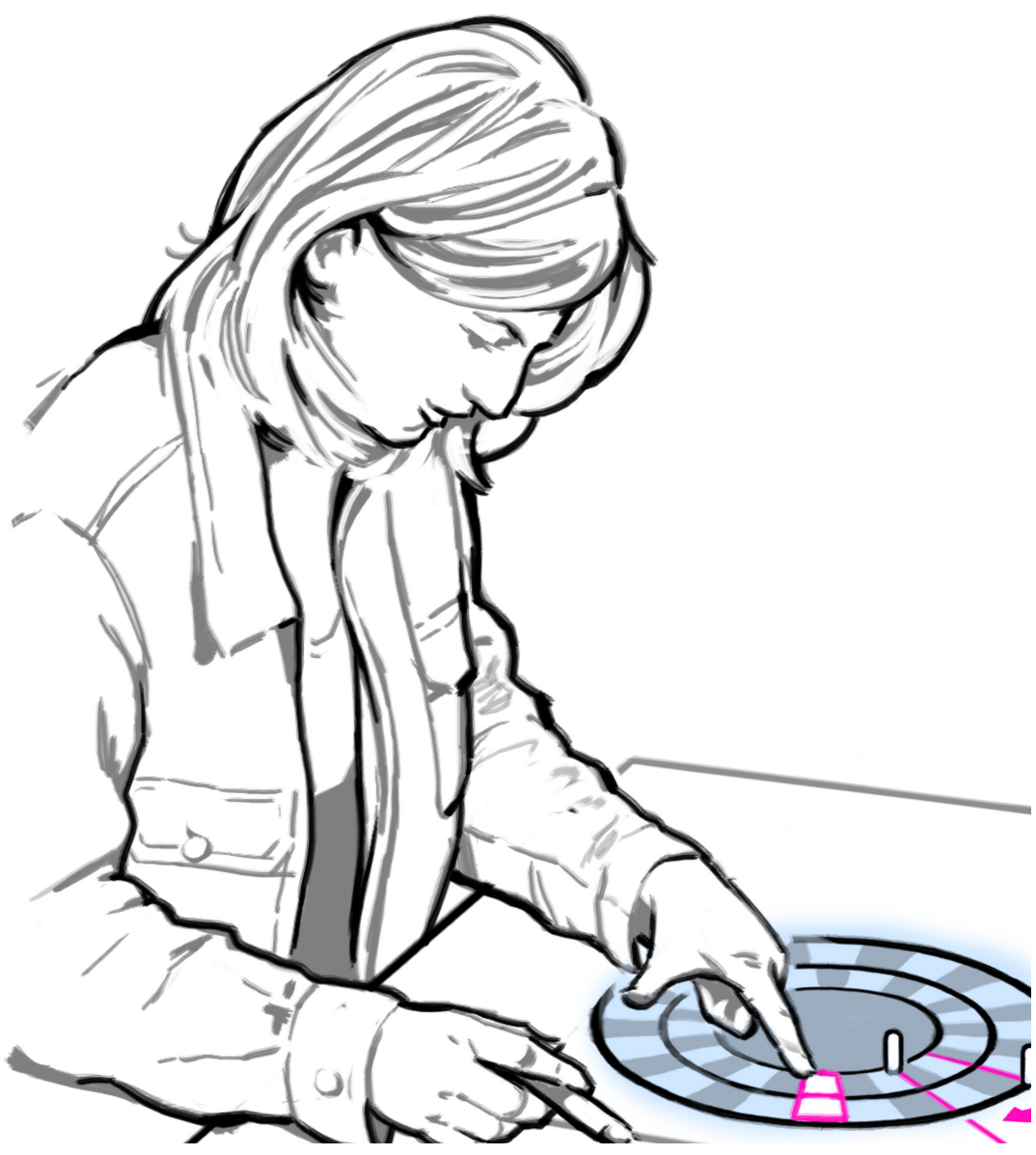
To do and notice:

Idea and Concept: Mathematikum Giessen (D)
"Text verschlüsseln_DEFI.indd"; Nr. 10440

Encoder un texte

la roue de César

Déjà au temps de César des informations étaient cryptées grâce à ces méthodes – mais parfois aussi rapidement décryptées.



A vous de jouer:

- *Les deux anneaux se laissent décaler l'un par rapport à l'autre de sorte que chaque lettre corresponde à une nouvelle lettre. Choisissez n'importe quelle position:*
- *Ecrivez un texte court (en lettres majuscules).*
- *Cherchez chaque lettre du texte d'origine (= texte en clair) sur l'anneau extérieur et notez la lettre correspondante sur l'anneau intérieur. Ainsi vous obtenez un texte crypté (= texte secret).*
- *Pour le déchiffrage, procédez dans l'ordre inverse, mais vous devez d'abord découvrir la position des anneaux!*
- *Demandez à un partenaire de déchiffrer le texte que vous avez crypté.*

Pour en savoir plus:

Idée et conception: Mathematikum Giessen (D)
"Text verschlüsseln_DEFI.indd"; Nr. 10440

Encoder un texte

la roue de César

Pour en savoir plus

Le «chiffre de César» est une technique de cryptage et probablement la variante la plus simple d'une substitution monoalphabétique de manière «monographique». Cela signifie que chaque lettre individuelle d'un message (texte en clair) est remplacée (substituée) par une autre lettre, en déplaçant l'alphabet normal d'un certain nombre de chiffres. Pendant un déplacement de quatre positions, un «A» devient un «E» - on appellerait cela une «clé D» (D = quatrième lettre).

Cette manière de crypter ne convient pas dans la pratique parce qu'il est trop facile de casser ce code. Dans chaque langue chaque lettre est employée avec une fréquence différente. Certains mots sont faciles à identifier à cause de leur longueur (par exemple des mots fréquents avec trois lettres: moi, lui, par…). Il faut donc prendre un mot fréquent comme «und» («et» en allemand). Ensuite on écrit toutes les possibilités de cryptage: UND --> VOE --> WPF --> ... (décalage des deux alphabets de 1,2,3…lettres). Au plus après 25 essais on trouve la clé puisqu'on trouve l'une des combinaisons dans le «texte secret». La longueur de la clé, un mot que l'on utilise beaucoup de nos jours est donc de seulement 5 bit.

Le cryptage peut être beaucoup plus sûr si l'on utilise d'autres signes (majuscules, minuscules, et caractères spéciaux) et si l'on change le décalage après un certain nombre de lettres. Exemple: après quatre lettres, on tourne l'un des disques d'autant de positions qu'indique le nombre π: 3 1 4 1 5 9 2 6 ...

Les techniques de cryptage modernes utilisent des clés nettement plus longues. Le cryptage selon l'AES que l'on tient toujours comme sûre est basée sur de clés d'au moins 128-256 bits. De telles techniques sont employées dans le Wireless LAN (des réseaux sans fils d'ordinateurs) et aussi dans la téléphonie par ordinateur. D'ailleurs il s'agit d'un cryptage symétrique – la même clé est utilisée pour crypter et pour décrypter. Cela signifie aussi que l'émetteur et le récepteur connaissent la clé.

En revanche, les cryptages de mails et la sécurité sur internet (https://….) sont basés sur des cryptages asymétriques qui travaillent avec des clés publiques et privées. La clé publique est rendue publique comme son nom l'indique. Tout autre utilisateur peut prendre cette même clé afin de crypter des messages pour le propriétaire de la clé.

La clé privée par contre est gardée secrète par son propriétaire. Elle lui sert à décrypter des messages (textes secrets) qu'on lui a envoyés cryptés par la clé publique.

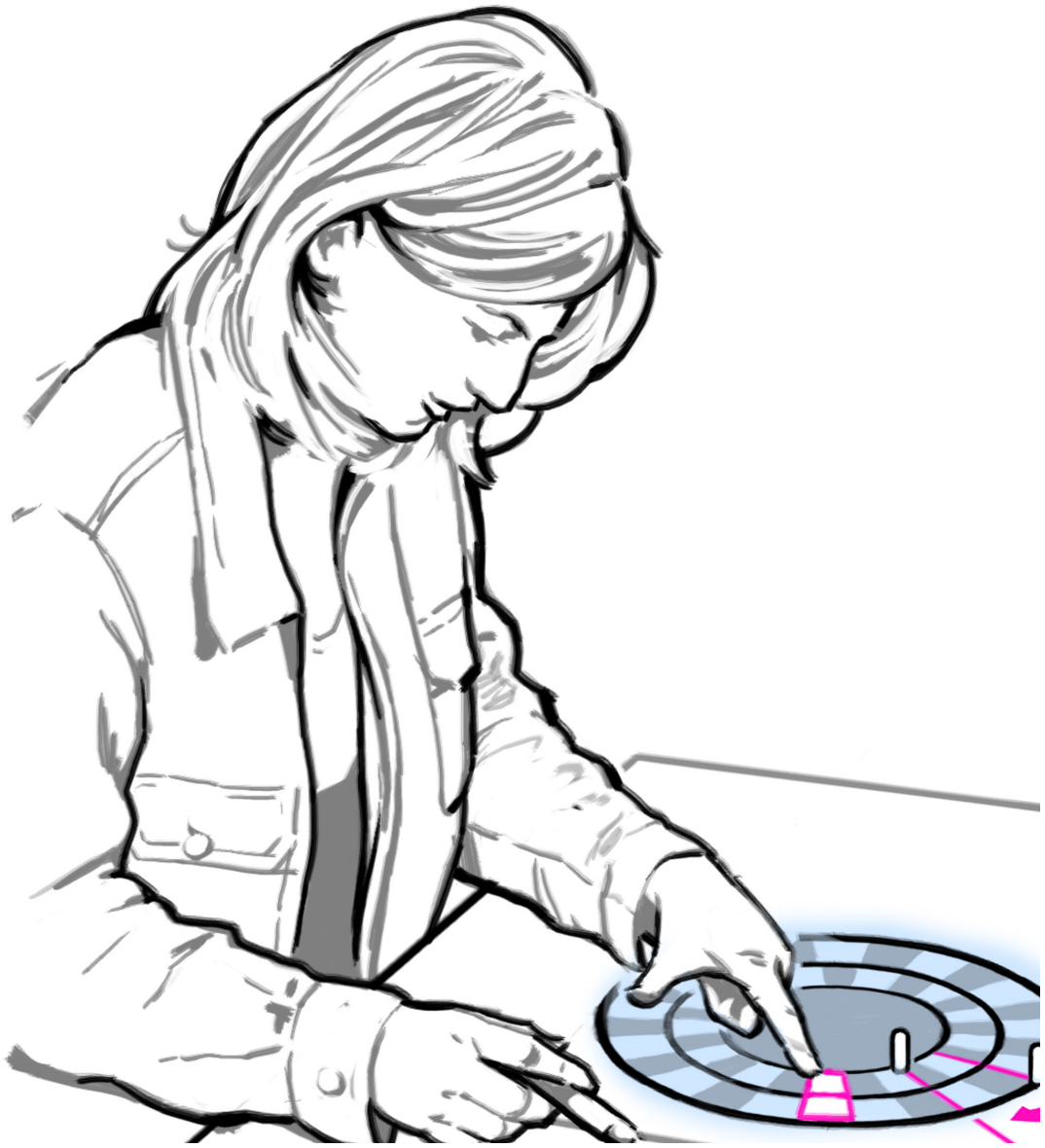
A vous de jouer:

Idée et conception: Mathematikum Giessen (D)
"Text verschlüsseln_DEFI.indd"; Nr. 10440

Cifrare un testo

La ruota di Cesare

Con questo sistema si cifravano i testi anche al tempo di Giulio Cesare. Spesso però risultava altrettanto facile decifrarli.



Che cosa fare:

- *I due cerchi si possono girare l'uno in senso opposto all'altro, in modo che ogni lettera può essere riferita a un'altra lettera. Disponeteli a piacimento:*
- *Scrivete un breve testo (in stampatello).*
- *Ora cercate ciascuna lettera del testo originale (= messaggio in chiaro) sul cerchio esterno e annotate le lettere corrispondenti del testo interno. Così otterrete il testo cifrato (= messaggio in codice).*
- *Quando si tratterà di decifrare, procederete inversamente, ma dovrete anzitutto scoprire la posizione originaria degli anelli!*
- *Sfidate qualcuno a decifrare un messaggio che avete appena cifrato!*

Vuole saperne di più?

Ideazione e progetto: Mathematikum Giessen (D)
"Text verschlüsseln_DEFI.indd"; Nr. 10440

Cifrare un testo

La ruota di Cesare

Vuole saperne di più?

Dal punto di vista della crittografia, il cosiddetto cifrario di Cesare è la variante più semplice di una sostituzione monoalfabetica „monografica“. Questo significa che ogni singola lettera di un messaggio (testo in chiaro) viene sostituita da un‘altra lettera, ricavata in base a una trasposizione fissa di un certo numero di posti lungo la serie delle lettere dell‘alfabeto. Uno spostamento di quattro posizioni fa sì che da una „A“ si ottenga una „E“: in questo caso si potrebbe parlare di „chiave D“ (in quanto la D è la quarta lettera).

Questo modo di cifrare non si adatta a scopi pratici perché è molto facile scoprire la chiave.

In ogni lingua infatti le varie lettere vengono usate con frequenze ben precise. Determinate parole sono molto facili da riconoscere a causa della loro lunghezza (per esempio spesso le parole hanno solo tre lettere: uno, gli, per, con, fra, ecc.). Si prenda per esempio una parola comune come „una“. Poi se ne scrivano le possibili versioni cifrate: UNA --> VOB --> WPC --> ... (trasposizione dei due alfabeti di 1, 2, 3 lettere). Dopo al massimo 25 tentativi si sarà trovata la chiave dato che si sarà riconosciuta una di queste combinazioni nel „messaggio cifrato“. La lunghezza della chiave, una parola oggi spesso utilizzata, assomma perciò ad appena 5 bit.

La codifica può essere resa molto più sicura se si utilizza anzitutto l‘insieme completo dei segni disponibili (con numeri, segni particolari) e poi se si cambia, dopo un certo numero di lettere, il criterio di trasposizione. Per esempio: dopo quattro lettere si ruota uno dei dischi di tante posizioni equivalente al corrispondente numero di π: 3 1 4 1 5 9 2 6 ....

I moderni sistemi di transcodifica usano chiavi sensibilmente più lunghe. Quello che oggi viene considerato sicuro, detto AES, si basa su chiavi lunghe almeno 128-256 bit. Queste tecniche vengono impiegate nel caso delle Wireless LAN (comunicazioni via onde radio in una rete locale di computer) o anche nella telefonia computerizzata.

Del resto qui abbiamo a che fare con una codifica simmetrica: infatti la stessa chiave viene utilizzata per codificare e decodificare il messaggio. Questo significa anche che il mittente e il ricevente devono conoscere la chiave.

La codifica delle e-mail o i protocolli di sicurezza su internet (https://...) si basano su codifiche asimmetriche, che operano con chiavi private e pubbliche. La chiave pubblica viene divulgata, come dice appunto il nome. Ogni altro utilizzatore può usare questa chiave per codificare dei messaggi indirizzati al proprietario della chiave.

La chiave privata invece viene tenuta segreta dal proprietario. Serve a decifrare i messaggi cifrati con la chiave pubblica che ha ricevuto.

Che cosa fare:

Ideazione e progetto: Mathematikum Giessen (D)
“Text verschlüsseln_DEFI.indd”; Nr. 10440