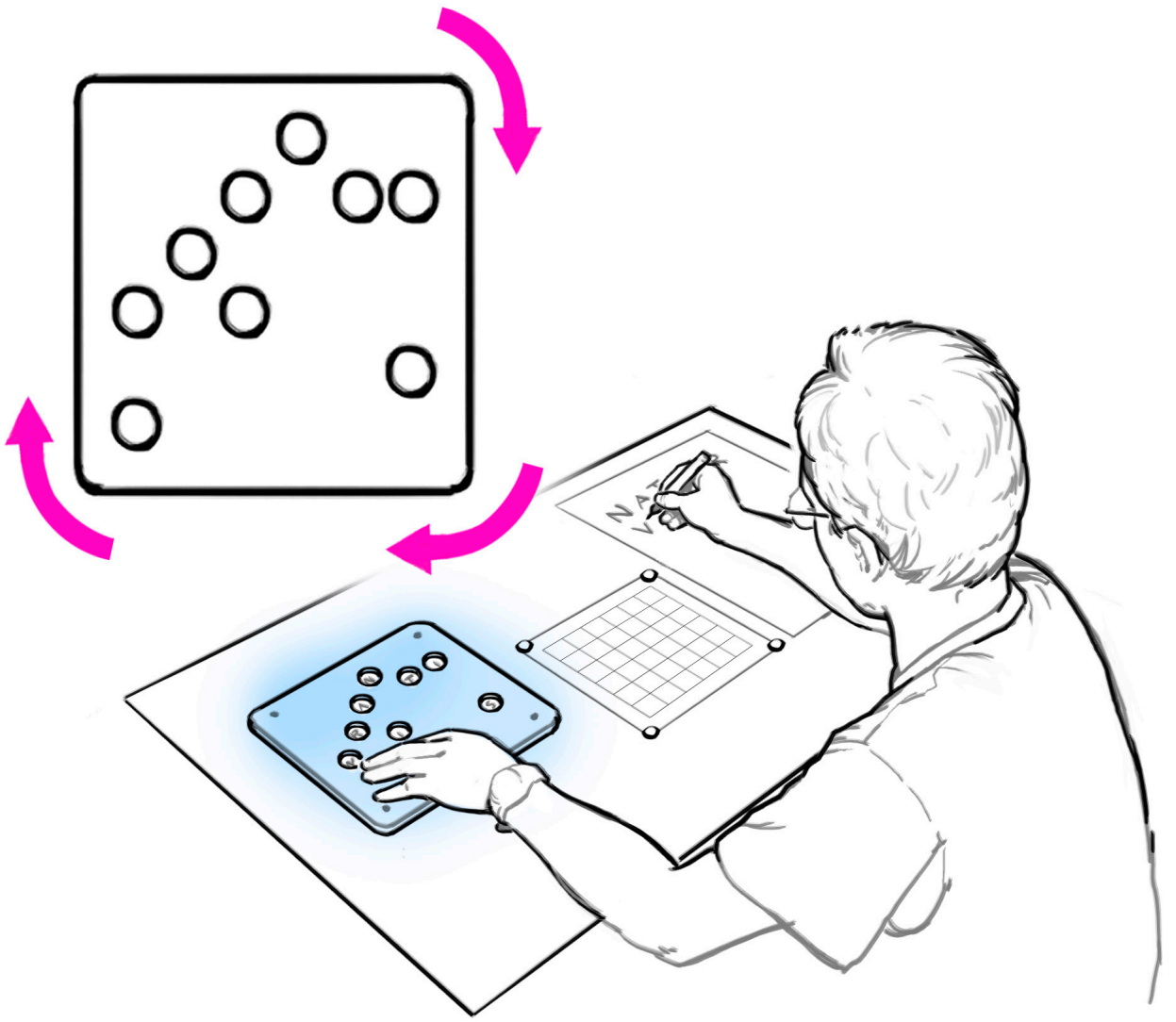
Krypto-Schablone

Hier handelt es sich um eine Verschlüsselungsmethode, die dem Rad Caesars (Exponat “Text veschlüsseln” auf der Rückseite des Tisches) weit überlegen ist!



Was tun und beachten:

- **Entschlüsseln:**
  Legen Sie die Krypto-Schablone auf das quadratische Feld links, das den Geheimtext enthält. Drehen Sie die Schablone so, dass sie in Position 1 liegt (Ziffer “1” steht senkrecht).

- *Lesen Sie die in den Löchern der Schablone erscheinenden Buchstaben zeilenweise von links oben nach rechts unten und übertragen Sie diese auf das Feld „Notizen“.*

- *Wenn Sie mit Lesen beim letzten Buchstaben angelangt sind, drehen Sie die Schablone auf Position 2. Lesen Sie weiter mit Position 2, dann mit Position 3 und 4.*

- **Die Anleitung zum Verschlüsseln finden Sie im Zusatzblatt.**

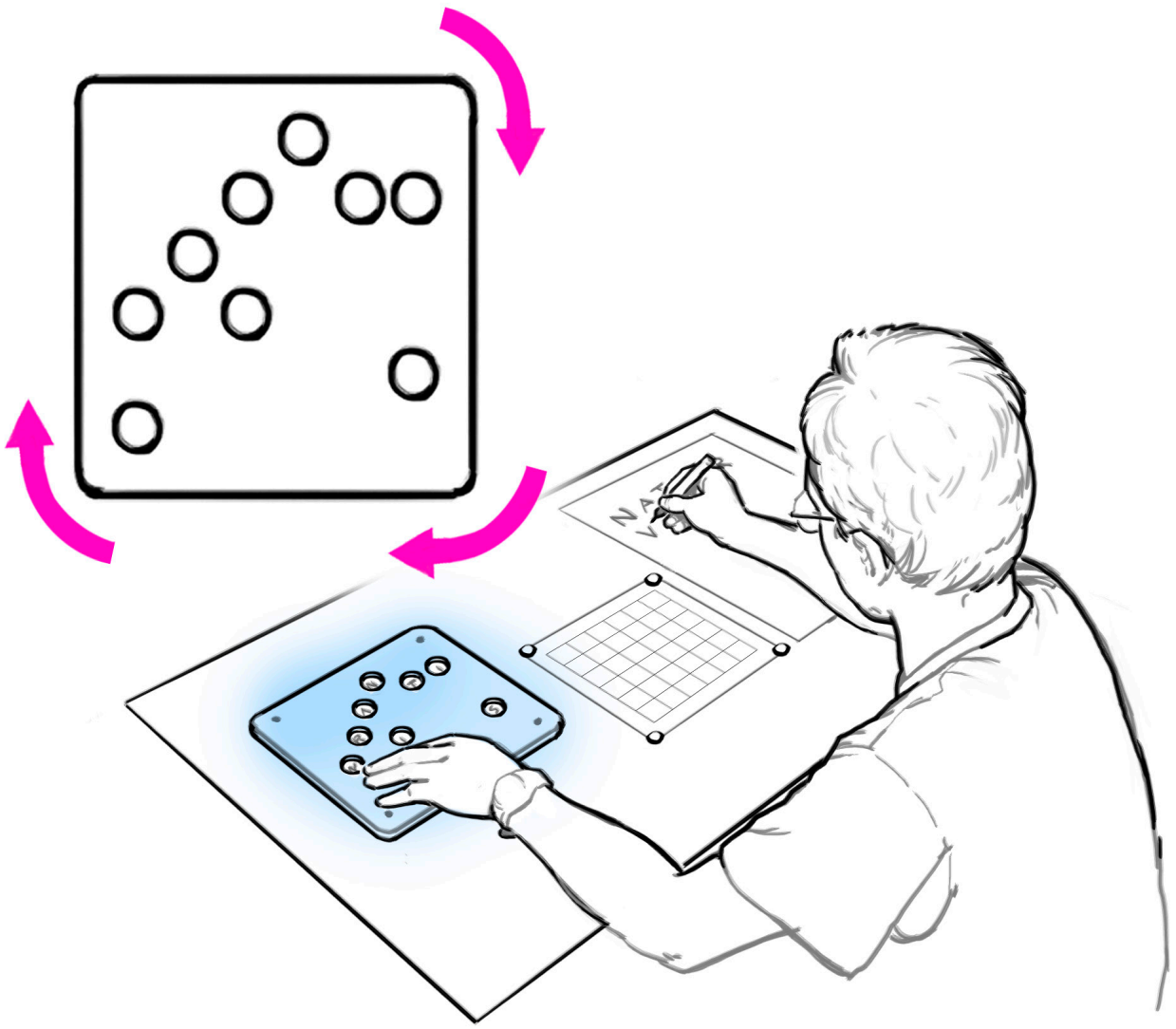
Wer mehr wissen möchte:

lesen Sie den Zusatztext

Konzept: Phänomenta Flensburg (D); Ausführung: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237

Krypto-Schablone

Hier handelt es sich um eine Verschlüsselungsmethode, die dem Rad Caesars (Exponat “Text veschlüsseln” auf der Rückseite des Tisches) weit überlegen ist!



Was tun und beachten:

- **Entschlüsseln:**
  Legen Sie die Krypto-Schablone auf das quadratische Feld links, das den Geheimtext enthält. Drehen Sie die Schablone so, dass sie in Position 1 liegt (Ziffer “1“ steht senkrecht).

- *Lesen Sie die in den Löchern der Schablone erscheinenden Buchstaben zeilenweise von links oben nach rechts unten und übertragen Sie diesen auf das Feld „Notizen“.*

- *Wenn Sie mit Lesen beim letzten Buchstaben angelangt sind, drehen Sie die Schablone auf Position 2. Lesen Sie weiter mit Position 2, dann mit Position 3 und 4.*

- **Die Anleitung zum Verschlüsseln finden Sie im Zusatzblatt.**

Wer mehr wissen möchte:

Konzept: Phänomenta Flensburg (D); Ausführung: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237

Krypto-Schablone

Wer mehr wissen möchte

Die Schablone muss natürlich so aufgebaut sein, dass beim Drehen erst nach 4 Drehungen ein schon besetztes Feld auftritt.

Für ein 6 x 6 Buchstabenschema wie hier gibt es 4^9 verschiedene Schablonen (262‘144). Wenn man die einzelnen Löcher der Schablone beliebig nummeriert und dann die Buchstaben in dieser Reihenfolge einträgt, sind es sogar etwa 95 Milliarden Möglichkeiten.

Für längere Texte könnte man also mit einem ganzen Satz von Schablonen arbeiten. Und dann die Reihenfolge der verwendeten Schablonen durch einen weiteren Schlüssel definieren: Bei zehn Schablonen könnte man dazu die Zahl Pi verwenden.

Beginnen Sie mit der Schablone (63. Nachkommastelle von Pi) und gehen Sie dann jeweils 17 Nachkommastellen weiter! Solch einer Verschlüsselung kommt man dann nur noch mit sehr ausgefeilten analytischen Methoden auf die Spur.

Übrigens eignet sich Pi besonders gut für solche Zwecke - die Anzahl Nachkommastellen sind unbegrenzt, die Nachkommastellen wiederholen sich nicht (kein Muster!) und man kann sehr viele Nachkommastellen von Pi inzwischen berechnen.

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 müssen.

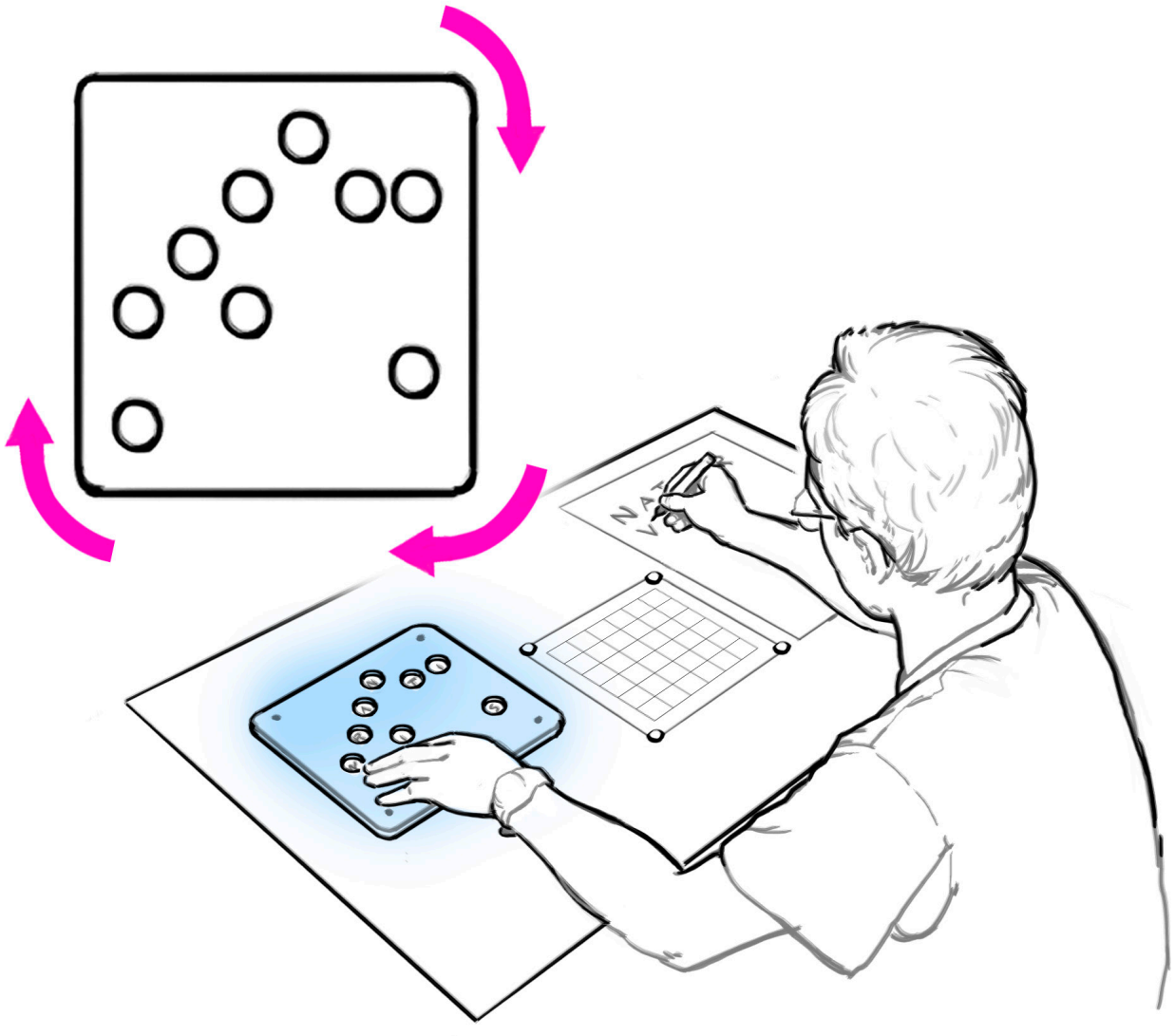
E-Mail-Verschlüsselung oder die Sicherheit im Internet (https://....) basieren demgegenüber auf asymmetrischen Verschlüsselungen, die mit privaten und öffentlichen Schlüsseln arbeiten. Der öffentliche Schlüssel wird, wie der Name sagt, öffentlich gemacht. Jeder andere Anwender kann diesen Schlüssel verwenden,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

Was tun und beachten:

Konzept: Phänomenta Flensburg (D); Ausführung: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237

Template Code

Here is a secret coding method a lot safer than Julius Caesar's method (see exhibit on the other side of the table).



To do and notice:

- **Decoding:**
  Put the template on the array of letters on the left, which contains the secret message. Turn the template so that it is in position 1 (the number 1 is upright).

- *Read the letters you see through the holes, starting at the top and going line by line, left to right, to the bottom. Write the letters in the plaintext space.*

- *Repeat, turning the template round to position 2, then 3, and finally 4.*

- **You can find a guide to this coding method on the Supplementary Sheet.**

Want to know more?

Concept: Phänomenta Flensburg (D); Realisation: Technorama
"Krypto-Schablone_DEFI.indd"; Nr. 10237

Template Code

Want to know more?

As a first requirement, the template has to be cut so that it will uncover all of the squares in the array in four turns. For a 6 x 6 array of letters as here, there are 4^9 different templates possible. If one numbers the holes randomly, and enters the message (plaintext) letters in that order, there are almost 100 billion possibilities!

For texts longer than 36 letters, one could work with a set of templates, and the order in which they are to be used hidden in another key: e.g. with ten templates, one could involve the number π.

Beginning with the template numbered the 63^{rd} digit of π after the decimal point, and then going 17 places further in π for the next template number. It would need an enormously elaborate system to crack this code!

π is a very useful choice for this purpose – the number of decimal places is infinite, there is no pattern in the digits within π , and you can choose any number of places after the decimal point for the template sequence.

Modern coding systems use appreciably longer keys. Totally secure systems based on the AES (Advanced Encryption Standard) use keys at least 128 bits long. These are used as standard in Wireless LAN (Local area networks linking computers) and computer telephony (CTI). As so far described, this is a symmetrical key system – the same key being used by the encoder and the decoder of the message.

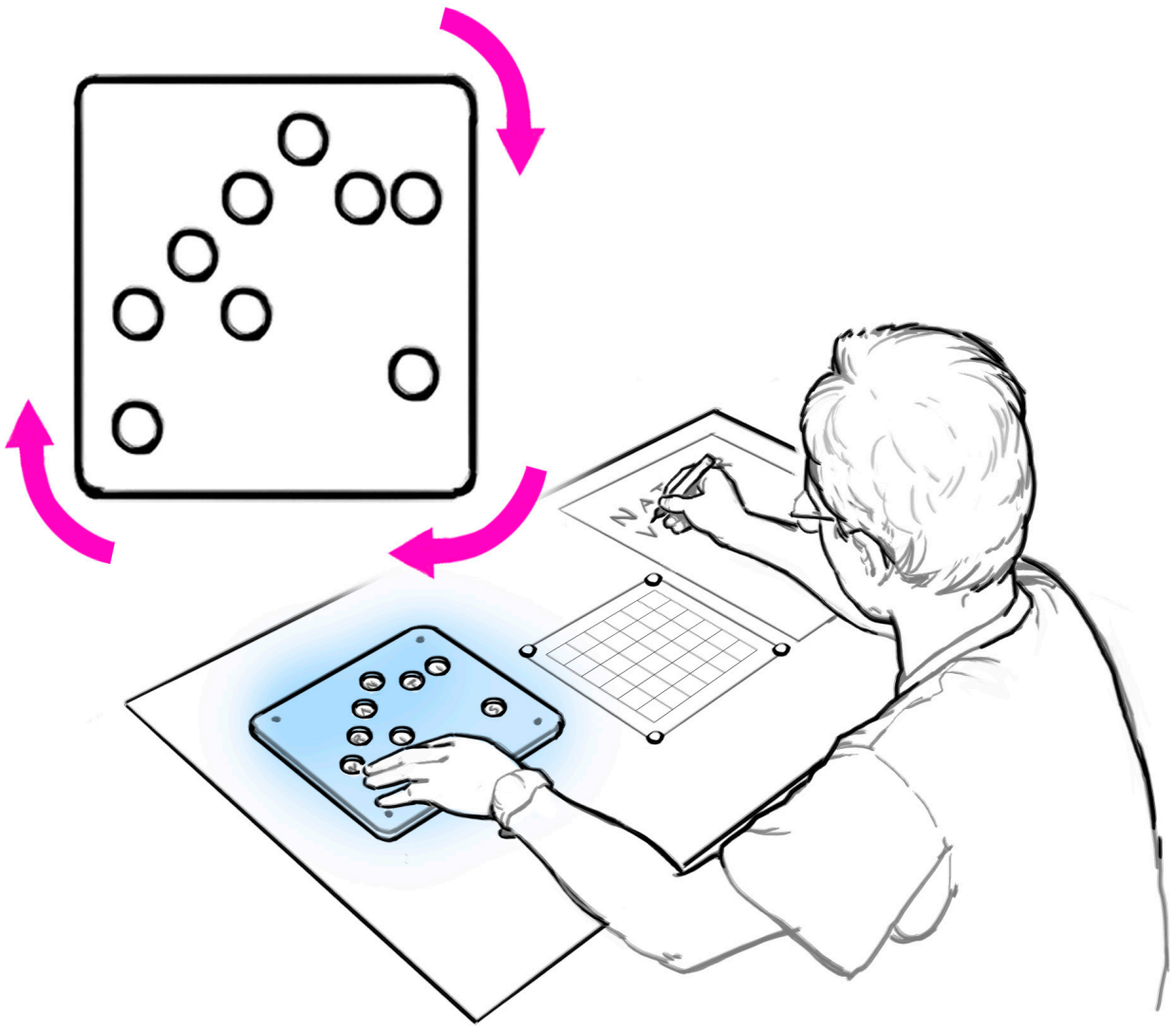
E-Mail and https://...(= hypertext transfer protocol secure) are based on asymmetrical keys, which operate with a public and a private key. A's public key, used for encoding, is known to all who send messages to recipient A. A, however, must use his private code to decode messages.

To do and notice:

Concept: Phänomenta Flensburg (D); Realisation: Technorama
"Krypto-Schablone_DEFI.indd"; Nr. 10237

Crypto-pochoir

Il s’agit d’une méthode de cryptage supérieure à la roue de César (voir l’expérience “crypter un texte” à l’arrière de la table).



A vous de jouer:

- **Décoder:**
  Mettez le crypto-pochoir sur le champ quadratique à gauche qui contient le texte secret. Faites pivoter le pochoir jusqu’à ce qu’il se trouve dans la position 1 (le chiffre «1» est vertical).

- *Lisez les lettres de chaque ligne apparaissant dans les trous du pochoir, d’en haut à gauche vers le bas à droite, et transposez les vers le champ de texte.*

- *Quand vous arrivez dans votre lecture à la dernière lettre, faites pivoter le pochoir dans la position 2. Continuez à lire avec la position 3, ensuite avec les positions 3 et 4.*

- **Vous trouverez l’instruction pour le cryptage dans le supplément.**

Pour en savoir plus:

Conception: Phänomenta Flensburg (D); Réalisation: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237

Crypto-pochoir

Pour en savoir plus

Bien entendu, le pochoir doit être construit de sorte que seulement après 4 tours un champ déjà rempli apparaisse pendant le pivotement.

Pour un schéma de 6x6 lettres comme ici, il y a 4^9 pochoirs différents (262‘144). Quand on numérote les trous au hasard et on met ensuite les lettres dans cet ordre, il y a même environ 95 milliards de possibilités.

Pour des textes plus longs on pourrait donc utiliser toute une série de pochoirs. Et on pourrait définir l’ordre des pochoirs par une autre clé: si l’on a 10 pochoirs, on pourrait utiliser le nombre Pi pour cela.

Commencez avec le pochoir (63^{ième} chiffre après la virgule de Pi) et déplacez vous ensuite à chaque fois de 17 chiffres après la virgule! Un tel cryptage ne peut être découvert qu’avec des méthodes d’analyse sophistiquées.

D’ailleurs Pi se prête particulièrement bien à cette fin – le nombre de chiffres après la virgule est infini et les chiffres après la virgule ne se répètent pas (aucune régularité) et on peut calculer vraiment beaucoup de chiffres après la virgule à l’heure actuelle.

Des méthodes d’encodage modernes utilisent des clefs nettement plus longues. L’encodage que l’on pense être inviolable se base selon AES sur des clefs d’au moins 128-256 bits. Ces techniques sont utilisées pour le Wireless LAN (des réseaux de communication d’ordinateurs) ou pour la téléphonie via ordinateurs.

Il s’agit d’ailleurs d’un encodage symétrique – la même clef est utilisée pour encoder et décoder. Mais cela signifie aussi que l’émetteur et le receveur doivent connaître la clef.

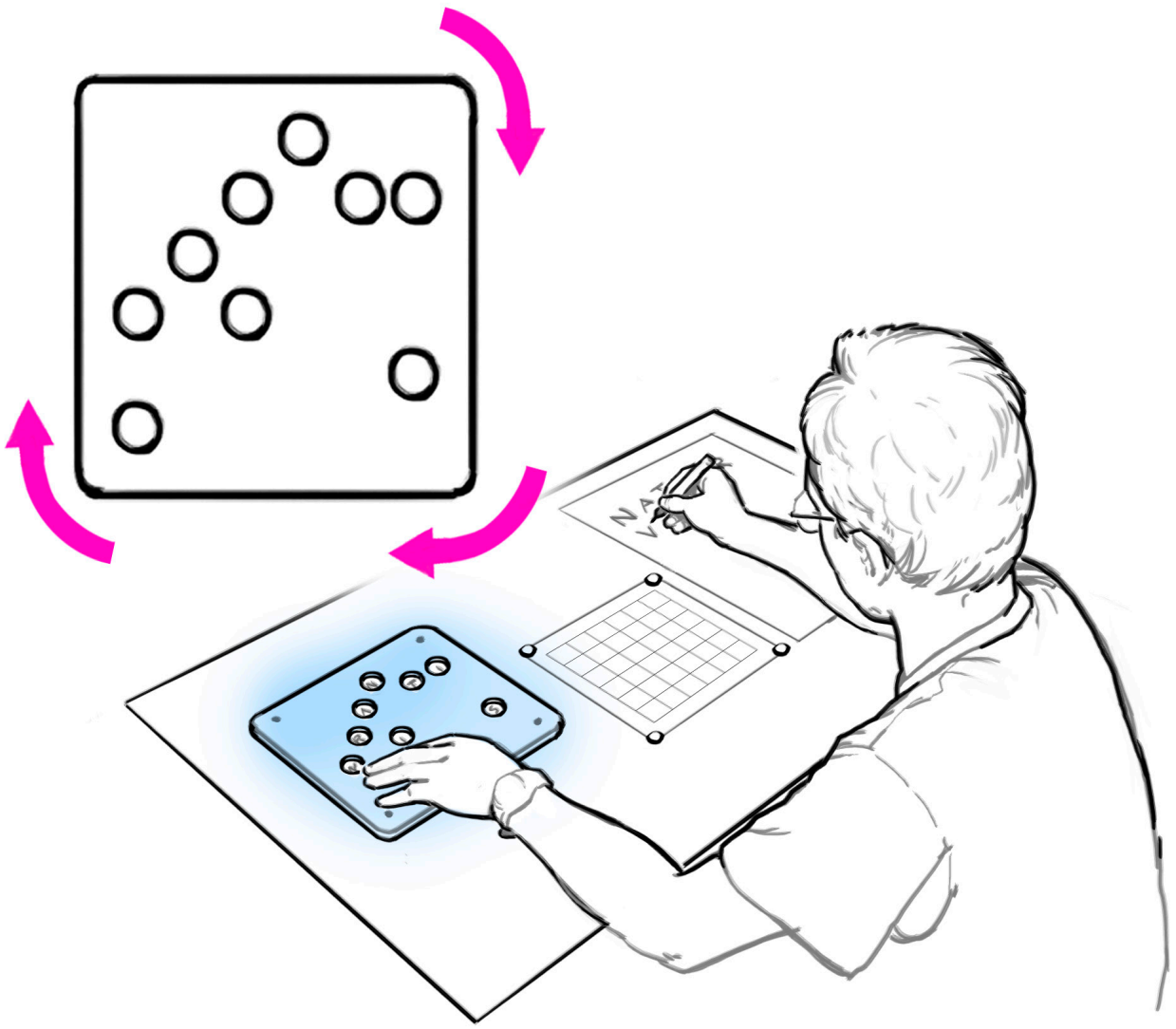
Les encodages d’emails ou la sécurité sur internet (https://…) se basent par contre sur des encodages asymétriques qui travaillent avec des clefs privées et publiques. La clef publique est rendue publique comme l’indique son nom. Chaque utilisateur peut utiliser cette clef pour encoder des messages pour le propriétaire de la clef.

A vous de jouer:

Conception: Phänomenta Flensburg (D); Réalisation: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237

Crivello crittografico

Si tratta di un metodo crittografico di gran lunga superiore a quello della „Ruota di Cesare“ (dall‘altra parte del tavolo)!



Che cosa fare:

- **Come decodificare:**
  Appoggiate il crivello (o maschera crittografica) sul campo quadrato a sinistra che contiene il testo cifrato. Ruotate il crivello in modo da posizionarlo nella posizione 1 (la cifra „1“ è verticale).

- *Leggete le lettere che compaiono nei fori, seguendo le righe da sinistra in alto verso destra in basso e riportatele sul riquadro del testo.*

- *Quando siete arrivati a leggere l‘ultima lettera, ruotate la maschera in posizione 2. Continuate a leggere nella posizione 2, poi passate alle posizioni 3 e 4.*

- **Sul foglio aggiuntivo troverete le istruzioni per la codifica supplementare.**

Vuole saperne di più?

Progetto: Phänomenta Flensburg (D); Realizzazione: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237

Crivello crittografico

Vuole saperne di più?

Il crivello (o maschera) deve essere fatto in maniera tale da permettere che un campo già visualizzato torni visibile solo dopo quattro rotazioni.

Per uno schema di 6 x 6 lettere come quello qui riprodotto, esistono 4^9 possibili maschere diverse (262 144). Se poi si numerano in modo arbitrario i fori della maschera e si trascrivono le lettere seguendo la sequenza prestabilita, le possibilità aumentano addirittura a 95 miliardi.

Per i testi più lunghi si potrebbe lavorare dunque con un‘intera serie di maschere. Inoltre si potrebbe definire la sequenza delle maschere da utilizzare per mezzo di un‘ulteriore chiave: se fossero dieci, per scegliere quella da usare si potrebbe utilizzare di volta in volta una cifra decimale del numero π.

Si cominci con lo schema corrispondente al 63° decimale di π e si prosegua risalendo di volta in volta di 17 decimali. Una codifica di questo genere può essere risolta solo utilizzando metodi analitici molto raffinati.

Il numero π è particolarmente adatto per questi scopi, in quanto il numero di decimali è illimitato e la loro sequenza non presenta ripetizioni (né regolarità), inoltre si può calcolare a piacimento il numero di decimali dopo la virgola.

I moderni metodi di codifica usano chiavi sensibilmente più lunghe. Quella che viene considerata valida in base ai requisiti AES si basa su chiavi lunghe almeno 128-256 bit. Queste tecniche vengono impiegate nelle Wireless LAN (reti locali tra computer che comunicano via radio) o anche nella telefonia computerizzata.

Del resto si tratta di 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.

Che cosa fare:

Progetto: Phänomenta Flensburg (D); Realizzazione: Technorama
“Krypto-Schablone_DEFI.indd”; Nr. 10237