RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

GEHEIMNIS

Auf Blei: Verflucht im Römischen Reich

In den Genen: Vererbte Krankheiten

Zwischen den Zeilen: Versteckte Botschaften

#35 Nr. 1 | 2025

Kryptografie

DER GEHEIME **DREH**

Leon Battista Alberti erfand im 15. Jahrhundert auf Wunsch des Papstes eine Chiffrierscheibe, mit der sich geheime Botschaften ver- und entschlüsseln ließen. Die revolutionäre Erfindung gibt bis heute Fragen auf.

„De Cyfris“ heißt eine kleine Abhandlung aus dem 15. Jahrhundert, in der sich eine geniale Erfindung versteckt. „Der Autor ist der erste, der das aus dem Arabischen stammende Wort ‚Cyfra‘ (ursprünglich: ‚leer‘) nicht für Zahl oder Ziffer verwendet, sondern für Chiffre: eine Verschlüsselung“, sagt Prof. Dr. Reinhold Glei, Inhaber des Lehrstuhls für Lateinische Philologie. Er hat sich mit der Schrift des italienischen Universalgelehrten Leon Battista Alberti (1404 – 1472) eingehend befasst. „Man kann überall lesen, dass er der Erfinder der Chiffrierscheibe war, aber meist wird nicht genau erklärt, was er da eigentlich erfunden hat und wie das funktionierte“, berichtet der Forscher.

Natürlich habe man schon immer versucht, Nachrichten zu verschlüsseln, auch bereits in der Antike. „Dafür hat man recht einfache Verfahren benutzt, zum Beispiel einen Buchstaben immer gegen einen anderen getauscht, der im Alphabet eine feste Anzahl Stellen weiter lag“, so Glei. Besonders sicher war diese Art der Verschlüsselung (Caesar-Chiffrierung) aber nicht. Einerseits kann man einfach ausprobieren, welcher Buchstabe für welchen anderen steht. Andererseits kann man auch anhand der Häufigkeiten der Buchstaben Rückschlüsse ziehen, um welche es sich im Klartext handelt. So kommen die Buchstaben e und s beispielsweise besonders oft in Texten vor. „Seit der Antike hatte es in Sachen Verschlüsselung erst mal erstaunlich wenig Fortschritte gegeben“, berichtet Reinhold Glei.

Revolutionäre Erfindung im Auftrag des Papstes

Erst Leon Battista Alberti machte eine revolutionäre Erfindung, und zwar im Auftrag des Papstes. „Der Papst war damals auch ein weltlicher Herrscher, der territoriale Ansprüche durchsetzen wollte, auch mit kriegerischen Mitteln“, erläutert Reinhold Glei. Daher hatte er ein Interesse daran, Nachrichten sicher zu verschlüsseln, um etwa militärische Operationen zu steuern.

Alberti als Universalgelehrter war mit dem päpstlichen Sekretär bekannt und bekam den Auftrag, eine neue Verschlüsselungsmethode zu entwickeln. Seine Methode basierte auf einem Hilfsmittel: der Chiffrierscheibe. Sie bestand aus einem fixen äußeren Ring, auf dem alle Buchstaben des lateinischen Alphabets plus vier Ziffern aufgetragen waren. Dabei handelte es sich sozusagen um einen öffentlichen ▸

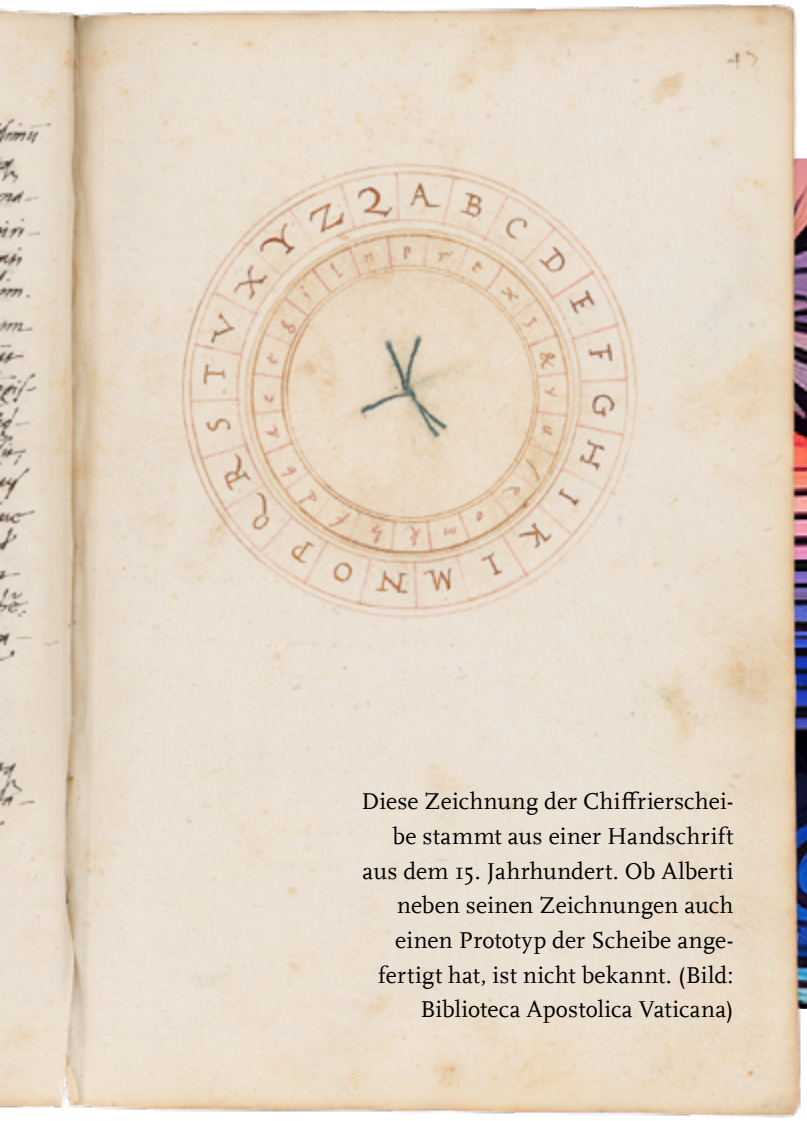
Auf der Chiffierscheibe kann man ablesen, welcher Buchstabe im Klartext gemeint ist. (Foto: tk)

Reinhold Glei ergründet die Geschichte der Kryptografie anhand von Jahrhunderte alten Handschriften. (Foto: tk)

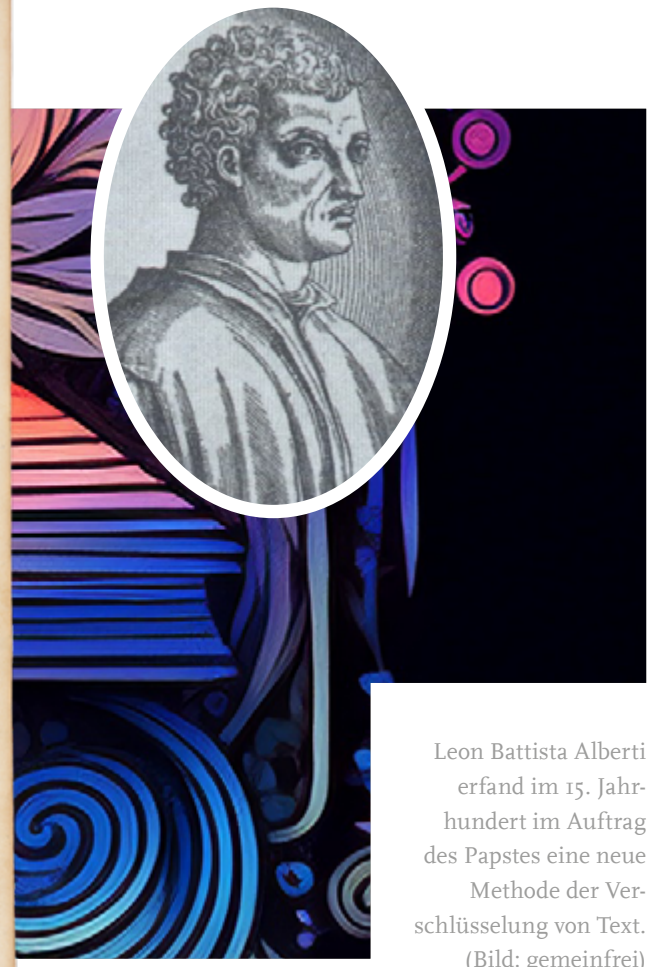
> „IM 16. JAHRHUNDERT GAB ES EINEN GEWISSEN BOOM DES INTERESSES AN VERSCHLÜSSELUNG.“
>
> Reinhold Glei

Schlüssel. Im Inneren lag ein weiterer, drehbarer Ring, der alle Kleinbuchstaben und ein Sonderzeichen enthielt, allerdings in unsortierter Reihenfolge. Diese innere Scheibe war individuell austauschbar, also ein privater Schlüssel.

Der Absender einer Nachricht ersetzte zur Verschlüsselung die Buchstaben des Klartextes, die er auf dem äußeren Ring ablas, durch die entsprechenden Buchstaben, die auf gleicher Höhe auf dem inneren Ring ablesbar waren. In unregelmäßigen Abständen drehte er den inneren Ring, sodass jeder Klartextbuchstabe nun eine andere Entsprechung hatte. Die Drehung des Rings wurde im verschlüsselten Text selbst durch sogenannte Steuerungsbuchstaben angezeigt. Angenommen, wir wollten den Namen ALBERTI verschlüsseln: Dazu wählen wir einen beliebigen Steuerungsbuchstaben, zum Beispiel o, und stellen ihn auf die I. Dann ergibt sich für A ein x, für L ein y, für B ein i; hier wechseln wir zum Beispiel zum Steuerungsbuchstaben k, sodass das folgende E jetzt ein r, das R ein s wird; schließlich wechseln wir zum Steuerungsbuchstaben x und erhalten für T ein o und für I ein g. Der chiffrierte Text ist also „oxyikrsxog“. „Da die Zuordnung der Buchstaben so ständig wechselt, kann man aus der Anzahl und Häufigkeit der Buchstaben keine Rückschlüsse mehr ziehen“, so Reinhold Glei. „Alberti war damit der erste, der eine Methode zur polyalphabetischen Verschlüsselung beschrieben hat.“ Weitere Verwirrung konnte man stiften,



Diese Zeichnung der Chiffrierscheibe stammt aus einer Handschrift aus dem 15. Jahrhundert. Ob Alberti neben seinen Zeichnungen auch einen Prototyp der Scheibe angefertigt hat, ist nicht bekannt. (Bild: Biblioteca Apostolica Vaticana)



Leon Battista Alberti erfand im 15. Jahrhundert im Auftrag des Papstes eine neue Methode der Verschlüsselung von Text. (Bild: gemeinfrei)

indem man Leerzeichen zwischen den Wörtern sowie Doppelbuchstaben wegließ und Großbuchstaben, Ziffern oder Sonderzeichen einfügte, die ohne Bedeutung waren, im obigen Beispiel etwa „oBxy!ik2rs%xYog“. „Wer nicht die gleiche Scheibe hatte wie der Absender, konnte einen solchen Text nicht entschlüsseln“, meint Glei. Eine sichere Sache also und eine geniale Erfindung. Aber so recht durchgesetzt hat sie sich trotzdem nicht.

Keine gute Gebrauchsanweisung

„Handschriftlich war die Schrift durchaus verbreitet, es sind heute 13 Abschriften bekannt“, berichtet Glei aus seinen Recherchen. Ob die Methode allerdings je zum Einsatz kam, ist nicht überliefert, auch nicht, ob Alberti neben seinen Zeichnungen auch einen Prototyp der Scheibe angefertigt hat. Im Text spricht er nur von „Formula“ (Schema), und in den Handschriften sind ganz unterschiedliche Scheiben abgebildet. Spätere Verschlüsselungen basierten auf anderen Systemen wie etwa Substitutionstabellen.

„Es könnte sein, dass man damals Albertis Methode einfach nicht so recht verstanden hat“, meint Reinhold Glei. „Der Text von Alberti ist teilweise kompliziert und auf knapp 20 Seiten kondensiert – eine gute Gebrauchsanweisung ist das nicht. Vielleicht war auch der Papst, der nur wenig Latein konnte, ‚not amused‘.“ Zudem muss es zeitaufwändig gewesen sein, Texte mit der Methode zu ver- und entschlüsseln. Für längere Texte war sie daher nicht geeignet.

Ein weiterer möglicher Nachteil: Sender und Empfänger benötigen zwingend den gleichen Schlüssel, sprich die gleiche Chiffrierscheibe, insbesondere den gleichen inneren Ring. „So einen Schlüssel muss man erst einmal sicher ans Ziel bringen“, so Glei, „und wehe, wenn er in falsche Hände gerät.“ Diebstahl, Erpressung oder gar Foltermethoden waren gang und gäbe – ein Risiko.

Reinhold Glei, der eher durch Zufall auf das Thema Verschlüsselung gestoßen ist, hat dennoch Feuer gefangen und recherchiert weiter in der Geschichte der Kryptografie. Vielleicht wurde Albertis Erfindung zwar nicht direkt angewandt, aber von anderen Autoren zur Kenntnis genommen, möglicherweise sogar plagiiert? „Es könnte sein, dass sich auch in Werken zu anderen Themen Hinweise darauf verstecken“, sagt er. „Im 16. Jahrhundert gab es einen gewissen Boom des Interesses an Verschlüsselung – vielleicht ausgelöst durch Albertis Erfindung?“ Dabei kamen allerdings vorwiegend Fremdalphabete zum Einsatz; das größte Rätsel stellt ein Manuskript aus der Zeit um 1500 dar, das bis heute nie entziffert wurde und in einem unbekannten Alphabet geschrieben ist. Ob es auf Albertis Methode basierend verschlüsselt wurde, weiß man nicht. Aber es ist möglich.

md

REDAKTIONSSCHLUSS

Schon im 15. Jahrhundert dachten sich die Menschen trickreiche Lösungen aus, um Geheimnisse sicher weitergeben zu können, zum Beispiel die rechts abgebildete Chiffrierscheibe (mehr dazu ab Seite 26). Mit ihr konnte man einen Klartext in Kauderwelsch verwandeln, indem man die Buchstaben des Klartextes auf dem äußeren Ring durch die Buchstaben auf dem inneren Ring ersetzte. Der innere Ring war drehbar. Um einen verschlüsselten Text zu entschlüsseln, musste man wissen, wie der innere Ring auszurichten ist. Die Ausrichtung wurde von sogenannten Steuerungsbuchstaben bestimmt, also Buchstaben, die keine Entsprechung im Klartext hatten, sondern nur dazu bestimmt waren, die Ausrichtung des inneren Rings anzugeben. War dieser richtig gedreht, konnte man den Klartext auf dem äußeren Ring ablesen.

LUST ZU KNOBELN?

Dann inneren Ring der Scheibe ausschneiden und los geht's:

yuose&azmydbkofxczn&cdeuqmlitokhyds

Hinweise: Unser Beispiel ergibt einen Satz mit sechs Wörtern und beinhaltet acht Steuerungsbuchstaben. Steuerungsbuchstaben müssen auf das Z des äußeren Rings ausgerichtet werden. Der verschlüsselte Text in diesem Beispiel beginnt mit einem Steuerungsbuchstaben. Die anderen sieben Steuerungsbuchstaben sind zufällig im Text verteilt und können auch mitten im Wort auftreten. Immer wenn ein Zeichen aus unserem Kauderwelsch-Beispiel sich nicht in einen sinnvollen Buchstaben übersetzen lässt, handelt es sich um einen Steuerungsbuchstaben. Richten Sie dann den inneren Ring neu aus, indem Sie dieses Zeichen des inneren Rings auf das große Z des äußeren Rings drehen. Achtung: Da der Erfinder der Chiffrierscheibe Latein sprach, fehlt der Buchstabe U im äußeren Ring, der für unseren Lösungssatz erforderlich ist. Ein V im äußeren Ring kann sowohl ein U als auch ein V bedeuten. Viel Spaß!

Die Auflösung finden Sie unten links auf dieser Seite.

IMPRESSUM

HERAUSGEBER: Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

WISSENSCHAFTLICHER BEIRAT: Prof. Dr. Birgit Apitzsch (Sozialwissenschaft), Prof. Dr. Thomas Bauer (Fakultät für Wirtschaftswissenschaft), Prof. Dr. Elena Enax-Krumova (Medizin), Prof. Dr. Constantin Goschler (Geschichtswissenschaften), Prof. Dr. Markus Kaltenborn (Jura), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Günther Meschke (Prorektor für Forschung und Transfer), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Nils Pohl (Elektro- und Informationstechnik), Prof. Dr. Tatjana Scheffler (Philologie), Prof. Dr. Gregor Schöner (Informatik), Prof. Dr. Sabine Seehagen (Psychologie), Prof. Dr. Roland Span (Maschinenbau), Prof. Dr. Marc Wichern (Bau- und Umweltingenieurwissenschaft), Prof. Dr. Peter Wick (Evangelische Theologie)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Dr. Lisa Bischoff (lb); Raffaela Römer (rr)

FOTOGRAFIE: Damian Gorczany (dg), Schiefersburger Weg 105, 50739 Köln, Tel.: 0176/29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de; Tim Kramer (tk), Agentur für Markenkommunikation, Ruhr-Universität Bochum

COVER: RUB, Tim Kramer

BILDNACHWEISE INHALTSVERZEICHNIS: Teaserfoto für Seite 14: Roberto Schirdewahn; Seite 22, 62: RUB, Tim Kramer

GRAFIK, ILLUSTRATION, LAYOUT UND SATZ:
Agentur für Markenkommunikation, Ruhr-Universität Bochum, www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation. Die Illustrationen wurden mit Adobe Firefly erzeugt.

DRUCK: LD Medienhaus GmbH & Co. KG, Hansaring 118, 48268 Greven, info@ld-medienhaus.de, www.ld-medienhaus.de

ANZEIGEN: Dr. Julia Weiler, Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de

AUFLAGE: 3.900

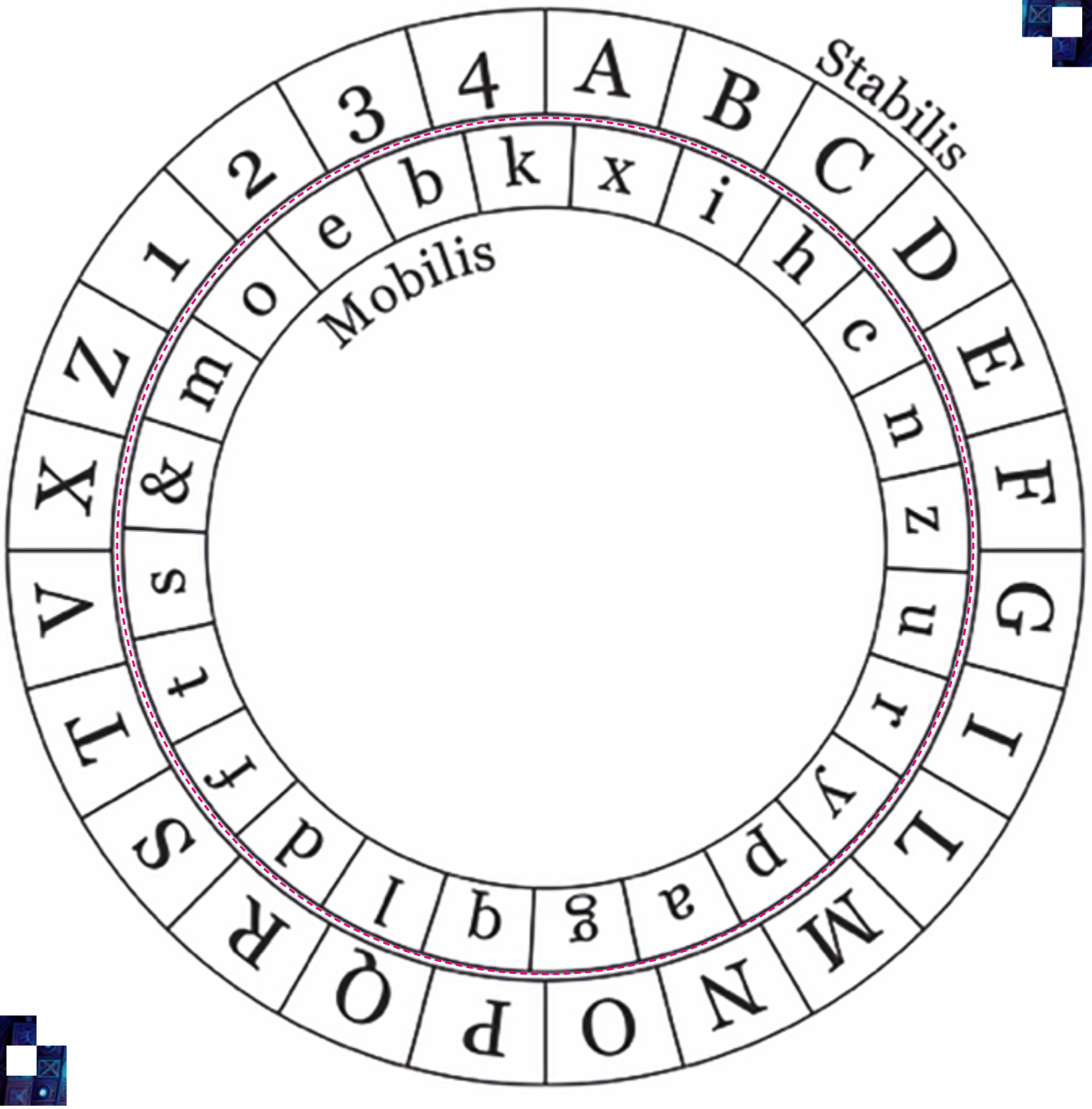
BEZUG: Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin/abo. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden.

ISSN: 0942-6639

Die nächste Ausgabe von RUBIN erscheint am 1. Dezember 2025.

Lösungssatz: Viel Freude beim Lesen von Rubin

CHIFFRIERSCHEIBE



Den inneren Ring der Scheibe ausschneiden und los geht's.