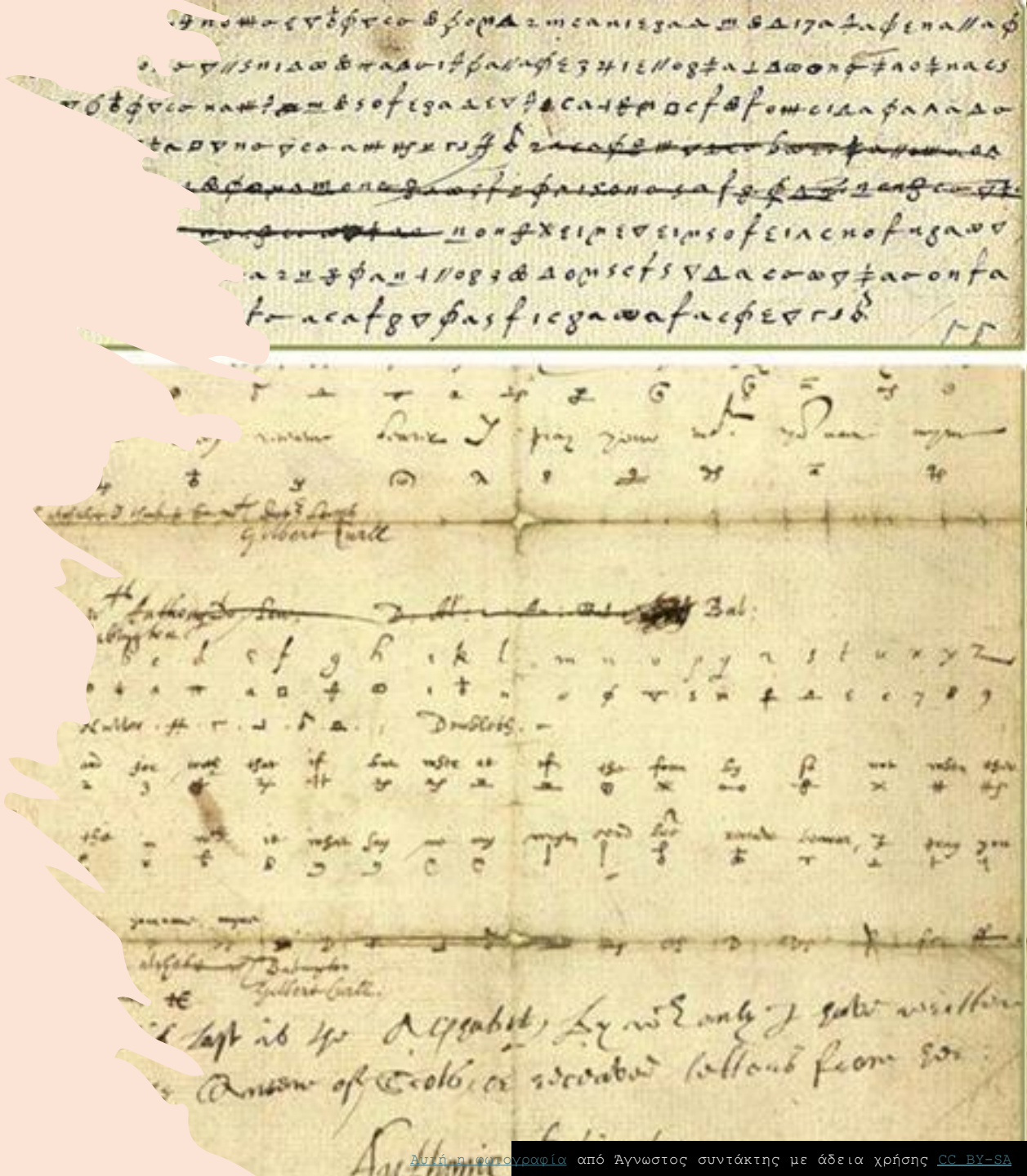
Die Geschichte der Geheimschrift und ihre Entwicklung bis zur heutigen Zeit



Referat : Angeliki Balla (1565202300051)
Seminarleiter: Prof. Joachim Theisen

Definition der Geheimschrift

Was ist Geheimschrift?

Geheimschrift ist die verschlüsselte oder unsichtbar gemachte schriftliche Wiedergabe der Wörter einer Sprache, sodass ein Text nur von den Leuten gelesen werden kann, die das Verschlüsselungssystem kennen oder wissen.

Die Ursprünge der Geheimschrift

- Notwendigkeit durch politische, militärische und religiöse Anforderungen.
- Diskretion und Sicherheit als Hauptziele.
- Erste Anwendungen in antiken Kulturen.

Steganographie – Verdeckten Botschaften

Nachrichten verstecken, nicht verschlüsseln

•**Definition**:

- *Steganographie*: Griechisch *steganos* (bedeckt) und *graphene* (schreiben).
- Ziel: Die Existenz der Nachricht selbst verbergen.

•**Historische Methoden**:

- Altes China:
  - Botschaften auf feiner Seide geschrieben, zu Wachskugeln geformt und verschluckt.
- Tithymalus-Pflanze:
  - Unsichtbare Tinte aus Pflanzensaft (Milch), die beim Erhitzen braun wird.
  - Spione nutzten Urin als Ersatz für unsichtbare Tinte, da er ähnliche Eigenschaften hatte.

Kryptographie

- **Definition:**

Kryptographie (kryptos – verborgen)

Ziel: Den Sinn der Nachricht durch Verschlüsselung verbergen, nicht die Nachricht selbst.

- **Unterschied:**

Steganographie: Existenz der Nachricht wird versteckt.

Kryptographie: Nachricht ist sichtbar, aber unverständlich ohne Schlüssel.

Hauptverfahren der Kryptographie:

Transposition:

Änderung der Buchstabenanordnung (z. B. Anagramme).

Substitution:

Ersetzung von Buchstaben durch andere (z. B. erste Erscheinung im Kamasutra, später Caesar-Verschlüsselung).

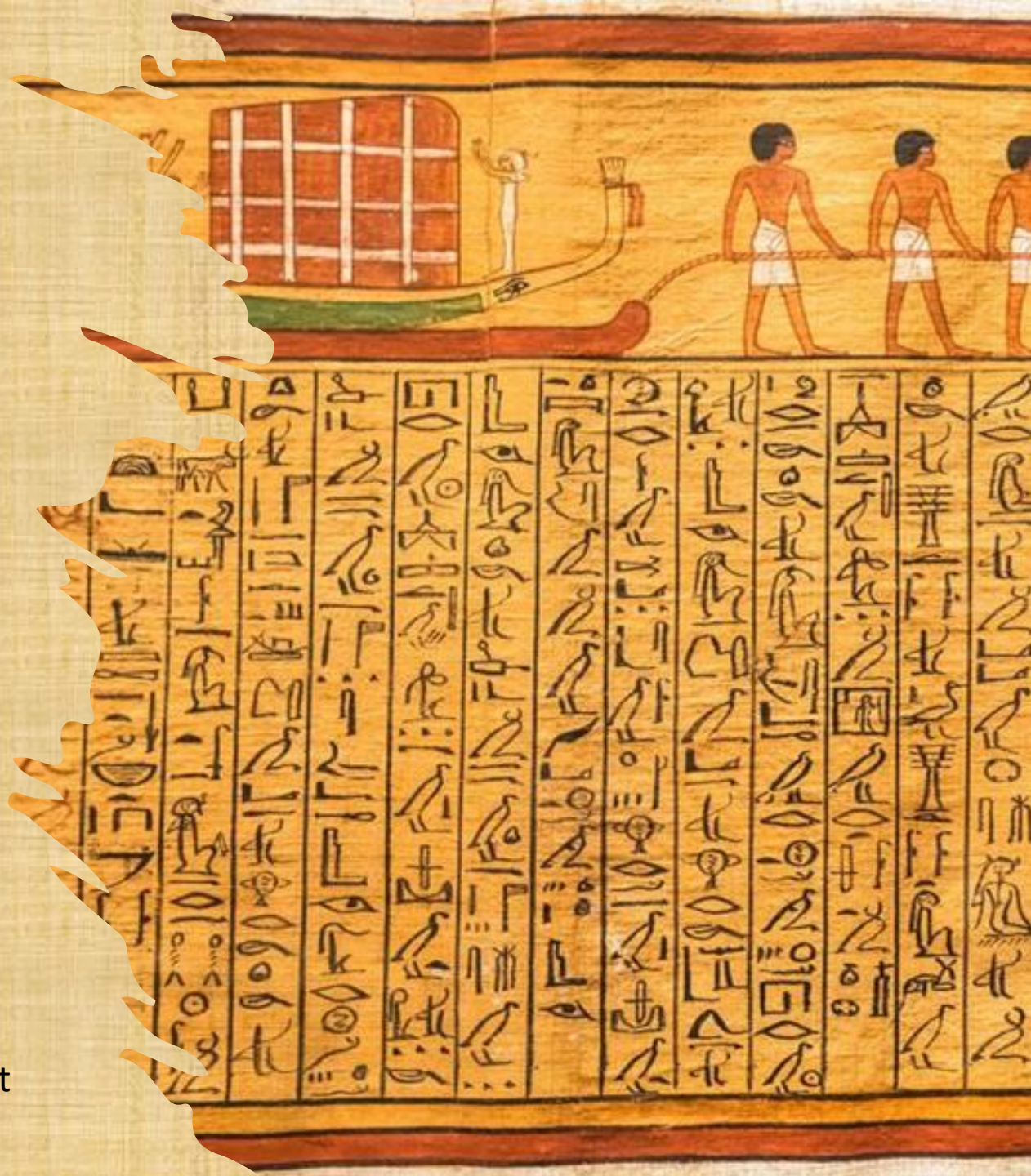
Ägyptische Geheimschrift

Geheimschrift im alten Ägypten

- 1900 v. Chr.: Einsatz spezieller Hieroglyphen in königlichen Grabinschriften.

Ziele:

- Schutz von Wissen.
- Bildung als Privileg der oberen Gesellschaftsschichten
- Erhalt eines Bildungsvorsprungs der Elite.
- Demonstration der Schreibfertigkeit.



Frühe Kryptographie

- Nachweisbar: Ägyptische Kryptographie als erste schriftliche Dokumentation.
- Unklarheit: Ob Kryptographie vor der Zeit der Ägyptern genutzt wurde.

Die Skytale

Verschlüsselung bei den Spartanern

•**Zeit**: Um 500 v. Chr.

•**Verfahren**:
- Zylindrischer Holzstab mit bestimmtem Durchmesser.
- Streifen aus Pergament, Stoff oder Leder um den Stab gewickelt.
- Geheimer Text entlang des Stabs geschrieben.

•**Lesbarkeit**:
- Nur mit einem identischen Stab lesbar.

•**Zweck**:
- Vertrauliche militärische Kommunikation.

Wachstafeln als Geheimschrift

Der Fall Demaratos

Überschrift: Warnung vor Xerxes' Invasion (480 v. Chr.)

•Hintergrund:

- Demaratos, ein griechischer Exilant in Persien, wollte Sparta warnen.
- Ziel: Heimliche Nachricht über die geplante Invasion von Xerxes.

•Methode:

- Wachs von einer Schreibtafel abgeschabt, Botschaft auf das Holz geschrieben.
- Tafel mit neuem Wachs bedeckt, sodass sie leer wirkte

•Entschlüsselung:

- In Sparta zunächst unbemerkt.
- Kleomenes' Tochter riet, das Wachs abzukratzen.

•Ergebnis:

- Nachricht entziffert, Griechen konnten sich vorbereiten.

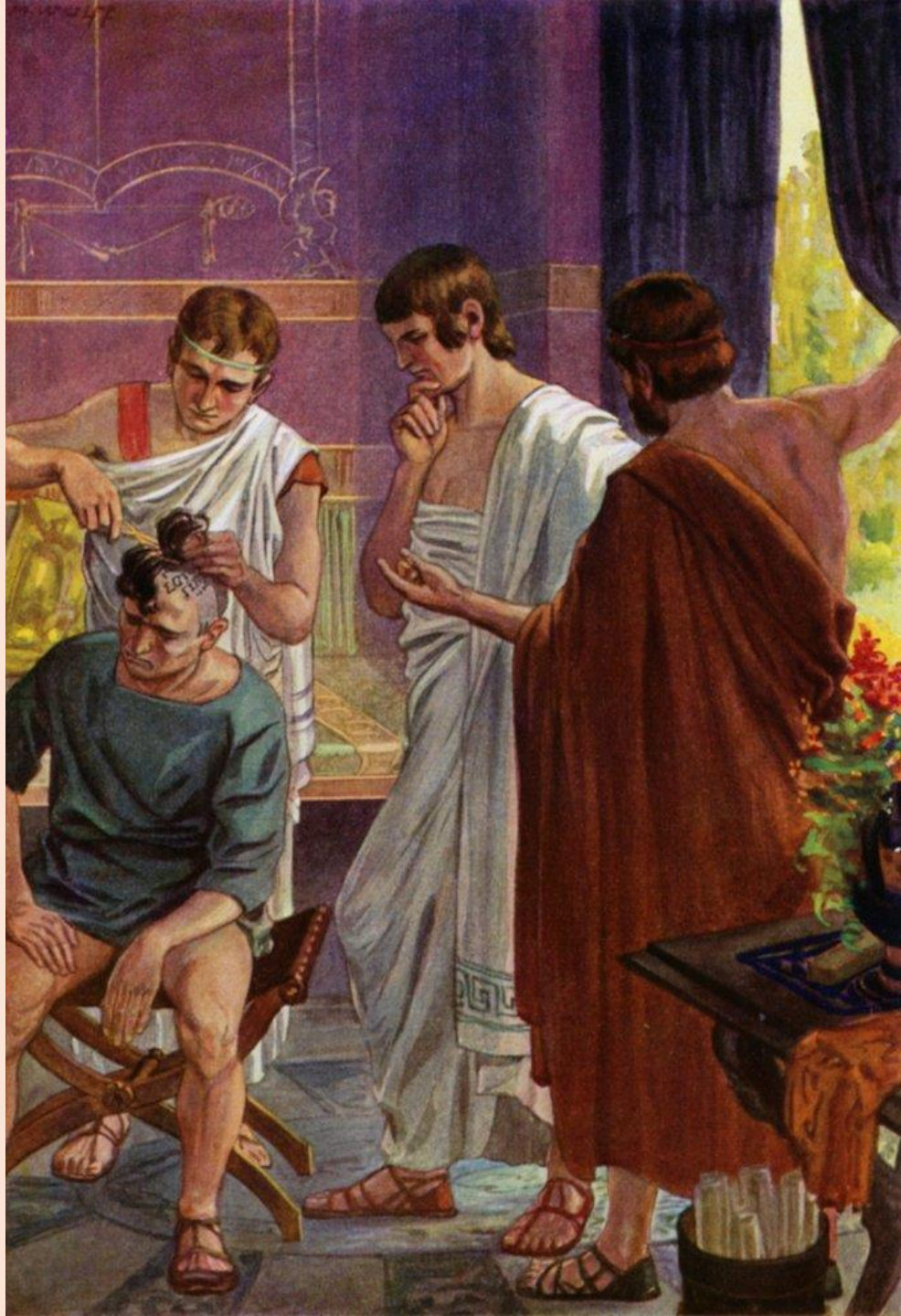
Eine außergewöhnliche Methode der Verschlüsselung (480 v. Chr.)

- **Hintergrund**:
  - Histiaeus, Tyrann von Milet, musste Aristagoras heimlich eine Nachricht übermitteln.

- **Verfahren**:
  - Kopf eines Sklaven rasiert und die Botschaft wird tätowiert oder eingebrannt.
  - Haare wuchsen nach, um die Schrift zu verdecken.

- **Übermittlung**:
  - Sklave reiste unauffällig zum Empfänger.
  - Beim Empfänger wurde der Kopf erneut rasiert, um die Nachricht zu lesen.

- **Zweck**:
  - Sicherstellung, dass die Botschaft geheim übermittelt wird.



Caesar Verschlüsselung (60 v. Chr.)

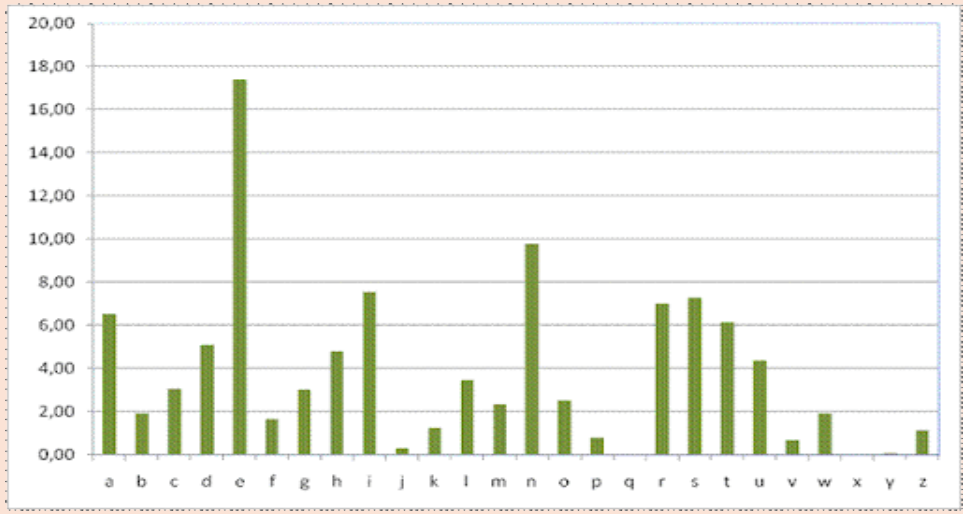
Klaralphabet (obere Reihe) und das Geheimalphabet in der unteren Reihe sahen bei Caesar folgendermaßen aus:

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

Verschlüsselt man z. B. das Wort **C A E S A R** mit dem Schlüssel 3 erhält man **F D H V D U**.

Die arabischen Kryptoanalytiker - Al-Kindi und die Häufigkeitsanalyse

Al-Kindi (801–873 n. Chr.), arabischer Philosoph und Wissenschaftler.



•**Wichtigstes Werk**:
- *Abhandlung über die Entzifferung kryptographischer Botschaften*.
- Erst 1987 im Süleyman-Archiv in Istanbul wiederentdeckt.

•**Methode der Häufigkeitsanalyse**:

- **Analyse eines Klartexts**:
  - Häufigkeit jedes Buchstabens in einem Text derselben Sprache ermitteln.
  - Buchstaben nach ihrer Häufigkeit ordnen (z. B. häufigster = "erster").

- **Analyse des Geheimtexts**:
  - Häufigkeit der Buchstaben im verschlüsselten Text bestimmen.
  - Vergleich mit den Mustern des Klartexts, um Buchstaben zuzuordnen

- **Ergebnis**:
  - Schrittweises Entschlüsseln monoalphabetischer Verschlüsselungen.

•**Einfluss**:
- Revolutionäre Methode, um Kryptographien zu brechen.
- Anwendung auch in theologischen Studien (z. B. chronologische Analyse religiöser Texte).

Die polyalphabetische Verschlüsselung – Alberti und Trithemius

Ein Meilenstein der Kryptographie

- **Leon Battista Alberti (1466): Begründer der Polyalphabetik und Autor des Buches** *De Componendis Cifris*

  - **Methode**:
    - Verwendete mehrere Geheimtextalphabete gleichzeitig.
    - Verschlüsselung: Jeder Buchstabe wurde abwechselnd aus unterschiedlichen Geheimtextalphabeten entnommen

    .
  - **Werkzeug**:
    - Alberti-Scheibe: Zwei drehbare Kupferscheiben.
      - Äußere Scheibe: Klartextalphabet + Ziffern (1–4).
      - Innere Scheibe: Geheimtextalphabet in zufälliger Reihenfolge.

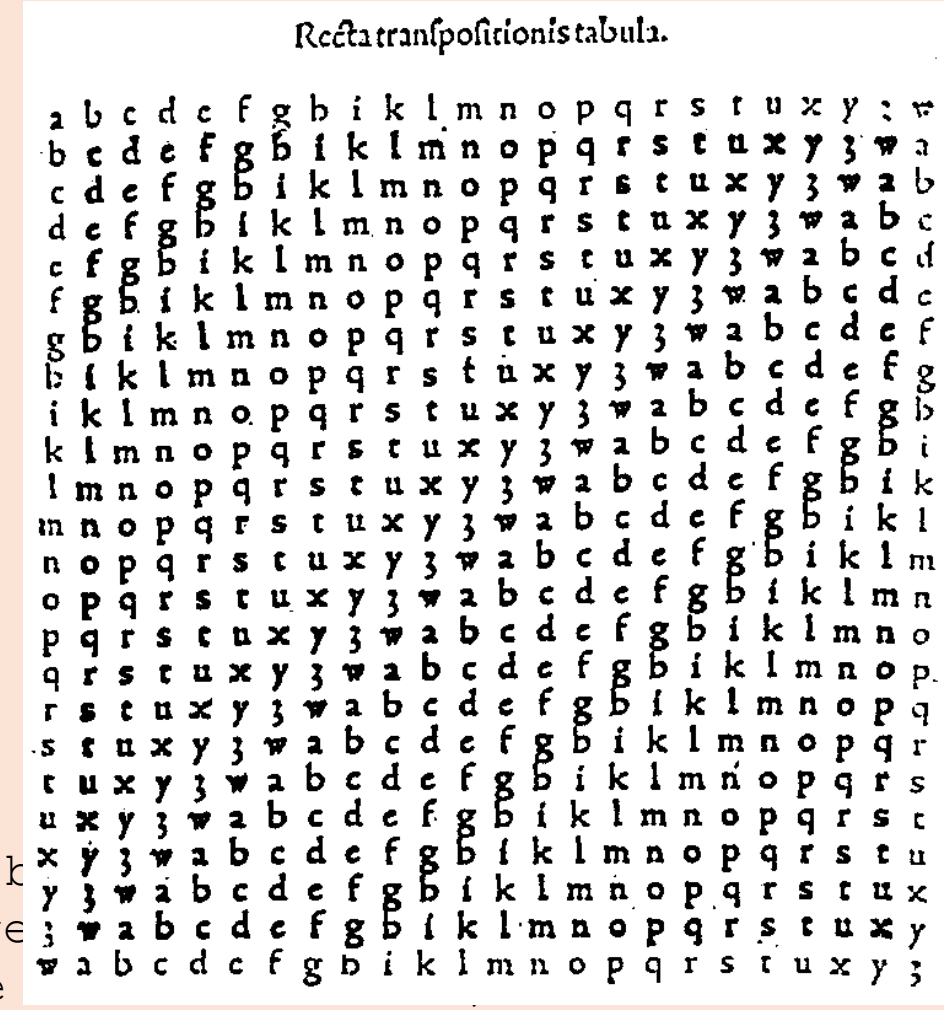
    - Schlüssel: Ein "Indikatorbuchstabe" gab die korrekte Ausrichtung der Scheibe vor.

Weiterentwicklung durch Johannes Trithemius (1518)

Vielseitige und mächtige Verschlüsselung

- **Erfindung der Tabula Recta**:
  - Tabelle mit 26 Geheimtextalphabeten.
  - Jedes Alphabet ist eine Caesar-Verschiebung
  - Ergebnis: Buchstaben im Geheimtext wechselten konstant zwischen den 26 Alphabeten.
  - Das erste bekannte polyalphabetische Verschlüsselungsverfahren

- **Anwendung**:
  - Genutzt in Diplomatie und Militär.
  - Galt über Jahrhunderte als unknackbar.



- **Vigenère:** Ähnlichkeit mit Trithemius
- **Unterschied:** Er setzt ein Schlüsselwort ein, das b
  welche Reihenfolge der Alphabete im Quadrat ge
- Vigenère erlaubt eine Anpassung durch variierende
  was die Entschlüsselung komplexer macht.

Entzifferung 1854 durch Babbage und Lösung im Jahre 1863 von Kasiski

Maria Stuart – Verschlüsselung in politischer Gefangenschaft

Verschlüsselung als Mittel der Kommunikation und des Widerstands

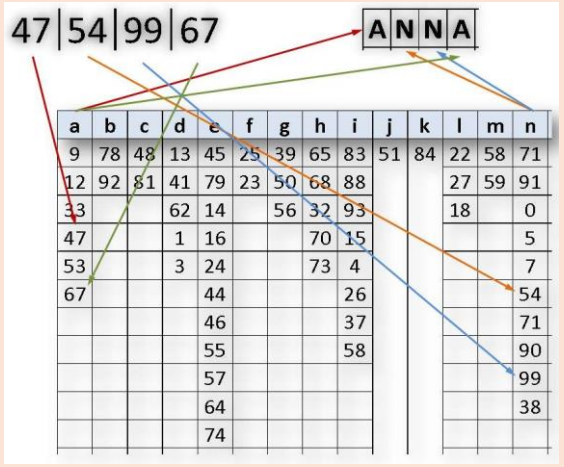
•**Historischer Kontext**:

- Gefangen von 1568 bis 1587 durch Königin Elisabeth I. von England.
- Kommunikation wurde vom Geheimdienstchef Sir Francis Walsingham überwacht.
- Überbringung von Nachrichten, z. B. versteckt in Bierfass-Spunden.

•**Verschlüsselungsmethoden**:

- **Caesar-Chiffre**:
  - Verschiebung von Buchstaben um eine festgelegte Anzahl von Stellen im Alphabet.

- **Homophone Verschlüsselung**:
  - Einem Buchstaben werden mehrere Symbole oder Zahlen zugeordnet.
  - Ziel: Sabotage der Häufigkeitsanalyse.
  - Beispiel: A = 12, 34, 56; B = 78, 90.



Tragisches Ende durch entschlüsselte Geheimschriften

• **Komplott:**

• Zusammenarbeit mit Anthony Babington, um Elisabeth zu stürzen.

• **Geheimdienstaktion**:

- Briefe wurden abgefangen und durch Walsinghams Experten entschlüsselt.
- Nutzung ihrer eigenen Methoden gegen sie.

•**Folge**:

- Überführung des Verrats.
- Prozess und Hinrichtung (1587).

•**Bedeutung**:

- Verschlüsselte Kommunikation als politisches Werkzeug und Risiko.
- Unterstreicht die wachsende Bedeutung der Kryptoanalyse in der Politik der Neuzeit .

Was waren Schwarze Kammern?

- Geheime Einrichtungen zur systematischen Entschlüsselung von Nachrichten.
- Dienten der Spionage und Informationsgewinnung in Europa.
- Höhepunkt: 17. und 18. Jahrhundert.

Ziele und Aufgaben:

- Öffnen und Entschlüsseln von diplomatischen und geheimen Briefen.
- Kopieren der Inhalte und Wiederherstellung der Briefe.
- Informationen an staatliche und fremde Mächte verkaufen.

Die Geheime Kabinetskanzlei in Wien war die disziplinierteste und schlagkräftigste Schwarze Kammer

- Ankunft der Briefe aus Botschaften.
- Siegel wurden vorsichtig geschmolzen.
- Stenographen fertigten Abschriften an.
- Briefe wurden in 3 Stunden wieder versiegelt und zurückgesandt.

Leistungen der Wiener Schwarzen Kammer:

- Herausragende Effizienz und Disziplin.
- Unschätzbares Material für die österreichischen Kaiser.
- Verkauf von Informationen an fremde Mächte – zusätzliche Einnahmequelle.

Kryptographie im späten 19. und frühen 20. Jahrhundert

- Nach der Entschlüsselung der Vigenère-Chiffre durch Charles Babbage (1854) und Friedrich Kasiski (1863) suchten Kryptographen nach sicheren Methoden.
- Herausforderung: Telegramme mussten vertraulich übertragen werden, um Informationen vor Industriespionage zu schützen.

Die Rolle von Guglielmo Marconi

- Entwickelte ein System zur drahtlosen Telekommunikation.

Errungenschaften

- Übermittlung von Wellen über weite Entfernungen.
- Kommunikation zwischen Schiffen, Truppen und Generälen ohne Kabel.

Problem:

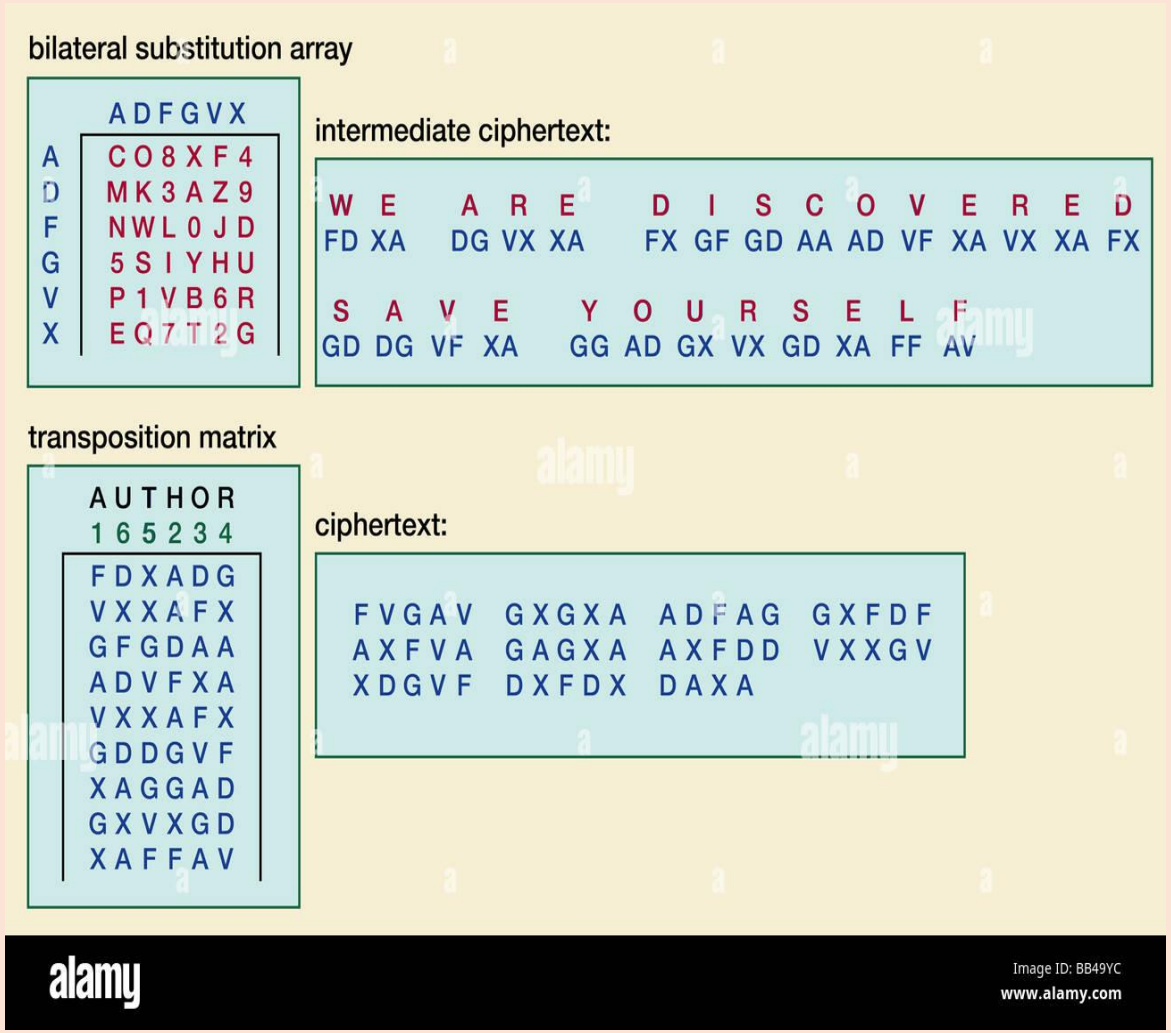
- Nachrichten konnten von Gegnern abgefangen werden → dringender Bedarf an Verschlüsselung.

Das ADFGVX-System im Ersten Weltkrieg

Erfinder: Funkoffizier Fritz Nebel.

Merkmale:

- Kombination aus **Substitution** und **Transposition**.
- Verschlüsselung mittels einer Tafel aus 36 Feldern:
  - Enthielt Buchstaben (A-Z) und Zahlen (0-9).
  - Benutzung von Koordinaten (A, D, F, G, V, X).
- **Verschlüsselungsstufen:**
  - Klarbuchstaben → Buchstabenpaare (z. B. "XG" = "Q").
  - **Transposition:** Neuordnung der Paare.
  - Bildung von Fünfergruppen für bessere Sicherheit.



Kryptographie im Zweiten Weltkrieg
Die Enigma-Maschine

Erfindung:

- Deutsche Chiffriermaschine, genutzt zur Verschlüsselung militärischer Nachrichten.
- Über 100.000 bis 200.000 Geräte wurden gebaut.

Technik:

- Rotorverschlüsselungsmaschine mit 3 Rotoren und einem Steckerbrett.
- Buchstaben wurden mehrfach vertauscht → hohe Sicherheit.
- Tagescodes: Entschlüssler benötigten tagesaktuelle Einstellungen der Maschine.

Knacken der Enigma:

- Britische Ingenieure erbeuteten eine Maschine mitsamt der Codeunterlagen.
- Alan Turing: Entwickelte die Turing-Bombe, mit der die Tagesschlüssel systematisch entschlüsselt werden konnten.
  → Entscheidender Beitrag zum Sieg der Alliierten.

https://youtu.be/5j09jnWQZqw?t=722

Der Mikropunkt (Zweiter Weltkrieg)

•**Technologie:**

- Spione verkleinerten Textseiten fotografisch zu Punkten mit weniger als 1 mm Durchmesser.
- Mikropunkte wurden in harmlos wirkenden Briefen versteckt, z. B. als Satzzeichen.

•**Nutzung:**

- Eingesetzt von deutschen Spionen in Südamerika zur Übermittlung von Informationen.
- Amerikanische Geheimdienste bekamen Hinweise, um Mikropunkte zu identifizieren.

•**Kombination mit Kryptographie:**

- Mikropunkte wurden verschlüsselt → erschwerte die Entzifferung durch Gegner

One-Time Pad (OTP) – Die "perfekte" Verschlüsselung

Definition und Grundprinzip:

One-Time Pad (Einmalverschlüsselung):

- Kryptographisches Verfahren der **polyalphabetischen Substitution**.
- Verschlüsselt jeden Buchstaben oder jedes Zeichen einer Nachricht durch ein einzigartiges Zeichen aus einem Schlüssel.
- Ursprünglich von Frank Miller für Telegrafenkommunikation vorgeschlagen.

Eigenschaften:

- **Zufälligkeit:** Der Schlüssel besteht aus rein zufälligen Zeichen.
- **Einmalige Verwendung:** Jeder Schlüssel wird nur für eine Nachricht verwendet und danach zerstört.
- **Länge:** Der Schlüssel ist mindestens so lang wie die Nachricht selbst.

Einsatz:

- Intensiv genutzt von Geheimdiensten wie CIA und KGB.
- Besonders verbreitet während des Kalten Krieges.

Internet-Erfindung (1989):

- Weit verbreitete Nutzung von Computern machte die Verschlüsselung notwendig
- Schutz von industriell-wirtschaftlicher und persönlicher Kommunikation

RSA-Verschlüsselung:

Entwicklung:

- Erfunden 1977 von Rivest, Shamir und Adleman.
- Asymmetrisches Verschlüsselungsverfahren.

Grundprinzip:

- Öffentlicher Schlüssel: Für alle zugänglich, dient zum Verschlüsseln.
- Privater Schlüssel: Nur dem Empfänger bekannt, dient zum Entschlüsseln.

Sicherheitsgrundlage:

- Beruht auf der Schwierigkeit, sehr große Zahlen in ihre Primfaktoren zu zerlegen.
- Ohne den privaten Schlüssel kann selbst ein abgefangener öffentlicher Schlüssel die Nachricht nicht entschlüsseln .

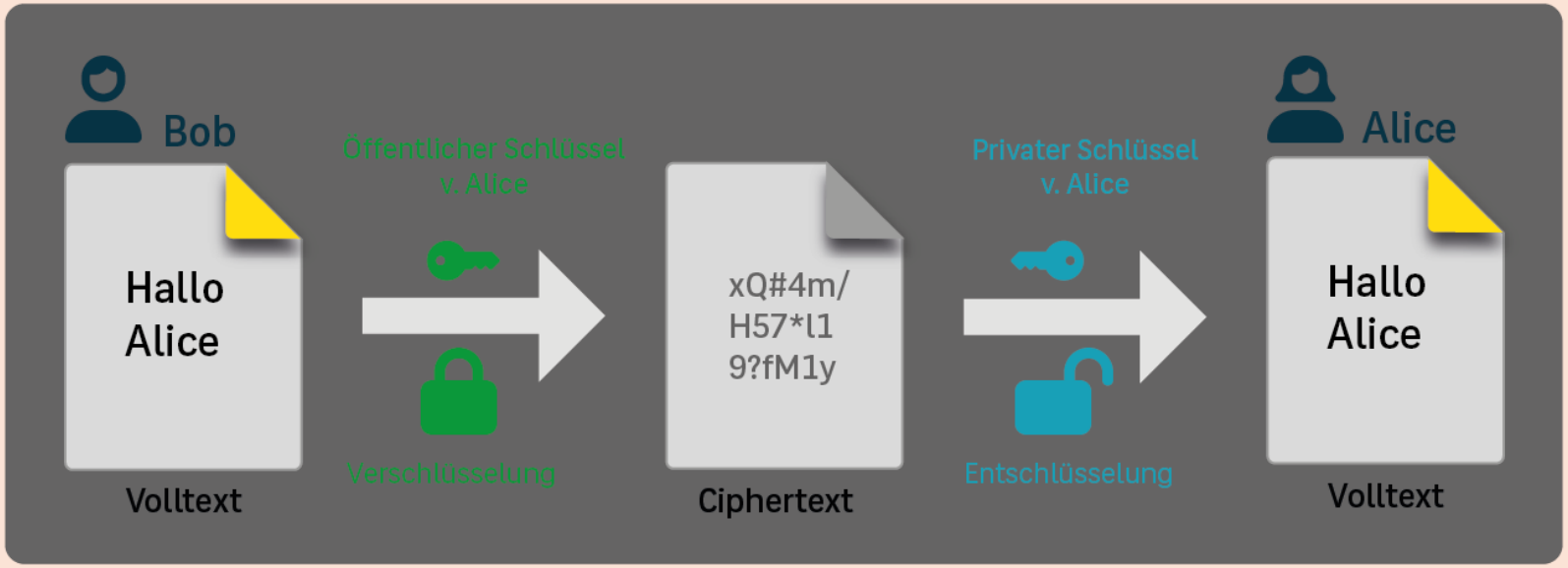
Das Alice-Bob-Modell

1. **Bob** erstellt ein Schlüsselpaar (öffentlich + privat).

2. **Bob** gibt seinen öffentlichen Schlüssel an **Alice** weiter.

3. **Alice** verschlüsselt ihre Nachricht mit Bobs öffentlichem Schlüssel und sendet sie zurück.

4. Nur **Bob** kann die Nachricht mit seinem privaten Schlüssel entschlüsseln.



Moderne Verschlüsselung im heutigen Alltag

Verschlüsselung ist allgegenwärtig und unbemerkt:

Internetnutzung: Bei jeder Verbindung über HTTPS, bei Messaging-Apps oder E-Mails.

Gerätekommunikation: Verschlüsselung wird bei Bluetooth, WLAN und Internet genutzt.

Wichtige Verschlüsselungstechnologien

- **PGP (Pretty Good Privacy):**
  Verschlüsselt E-Mails und garantiert, dass nur der beabsichtigte Empfänger sie lesen kann.

- **Neue Verfahren:**

  Komplexe mathematische Algorithmen sichern die Kommunikation ab.

Quanten-Computing: Bedrohung für die Zukunft von Cybersicherheit

Geheimschrift in der Literatur

Geheimschrift als literarisches Stilmittel

Beliebtheit

- Geheimschrift wird oft als Spannungselement verwendet, um die Handlung interessanter zu gestalten
- Die Dekodierung von Botschaften enthüllt entscheidende Wendungen und Geheimnisse.

Besonders populär in:

Thrillern, historischen Romanen und Detektivgeschichten

Bedeutende Autoren und Beispiele

Umberto Eco *Der Name der Rose*
Dan Brown *The Da Vinci Code*, *Angels and Demons*
Edgar Allan Poe war einer der ersten, der Kryptographie in Geschichten integrierte.

Literaturverzeichnis:

- Beutelspacher, A., Neumann, H. B., & Schwarzpaul, T. (2009). Kryptografie in Theorie und Praxis. Springer-Verlag.
- Grimm, R., Hundacker, H., & Meletiadou, A. (2008). Anwendungsbeispiele für Kryptographie.
- Singh, S. (1997). Geheime Botschaften. München: Deutscher Taschenbuch Verlag.
- Wrixon, F. (2000). Codes,Chiffren & andere Geheimsprachen. Köln: Könemann Verlagsgesellschaft mbH.

Bilderverzeichnis:

https://www.hnf.de/uploads/tx_templavoila/Skytale_HNF.jpg
https://upload.wikimedia.org/wikipedia/commons/thumb/3/34/Saepe_stilum_vertas_1.jpg/220px-Saepe_stilum_vertas_1.jpg
https://lernaufgaben.mebis.bycs.de/img/containers/uploads/posts/8/9/4/a/e/8bb34118-9339-4a42-afb9-ebe486dca608/folie2.png/e37733b8728f9eed05b7bb5facb3b1f3.webp
https://lh4.googleusercontent.com/proxy/0I6zFtE_R7WM9TLjfMqP_0ugT5fLrEA_8etgakdV3wQuWWH9G-p5ggmfefQMoPIQwPzmJ2goSa2N97whLoLDGrSY3ZFN05YHu1Q
https://i.etsystatic.com/15062905/r/il/6f0d23/1299674743/il_570xN.1299674743_i2a1.jpg
https://blog.gcwizard.net/wp-content/uploads/2021/01/Trithem.png
© Anna F. / Homofone Verschlüsselung / CC BY-SA 3.0 (Ausschnitt)
https://c8.alamy.com/compde/bb49yc/die-adfgvx-chiffre-von-der-deutschen-armee-im-ersten-weltkrieg-eingesetzt-bb49yc.jpg
https://youtu.be/5j09jnWQZqw?t=722
https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQh7xB-id7hsOQr_AollvvxTeVOEEWPonFSqg&s

Vielen Dank für Ihre Aufmerksamkeit !