Krypto (4V+2Ü)

8LP

Mo 10¹⁵ – 11⁴⁵
Mi 12¹⁵ – 13⁴⁵
Übungen: 16⁰⁰ – 17.30

} H20

Infos über Vorlesung:

- Instituts-Webseiten, → Lehre
- Rubikon

  rubikon.informatik.uni-ulm.de/course/169

1. Übungen am 18.4.

„Skript": Gescannte Aufschriebe

Buch: Kryptologie-Kompendium

Gute Bücher: Beutelspacher

Buchmann: Kryptographie

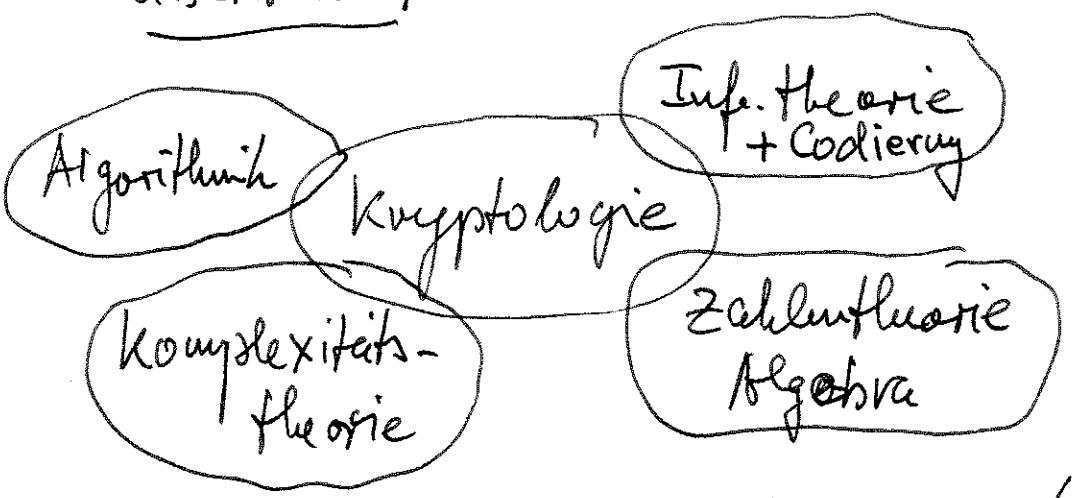
Wätjen: ″

Delfs/Knebl: Cryptogr.

Galbraith: Math of PK Crypto.

Paar/Pelzl: Understd. Crypto.

Überblick/Themen:



Bsp: $n (= p \cdot q)$
öffentl. geheim

Kryptologie

Kryptographie
(Algorithmen zum Ver-/Entschlüsseln, mit Schlüssel)

- klassisch (symm.)
- modern (asymm.)
- Hybrid

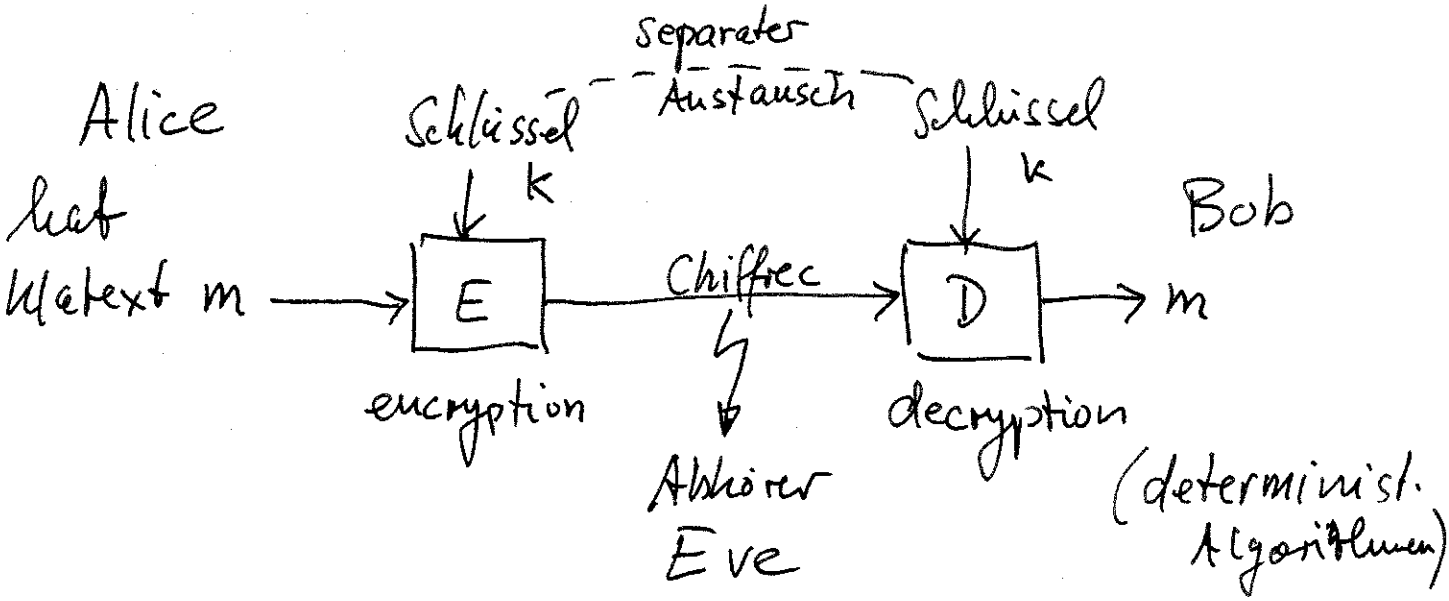
Kryptoanalyse
(Chiffre „knacken" – ohne Kenntnis des Schlüssels)

Algorithmen für
- Faktorisieren
- Diskreter Logar.

Begriffe:
- ciphertext only
- known plaintext
- chosen plaintext
- man-in-the-middle attack

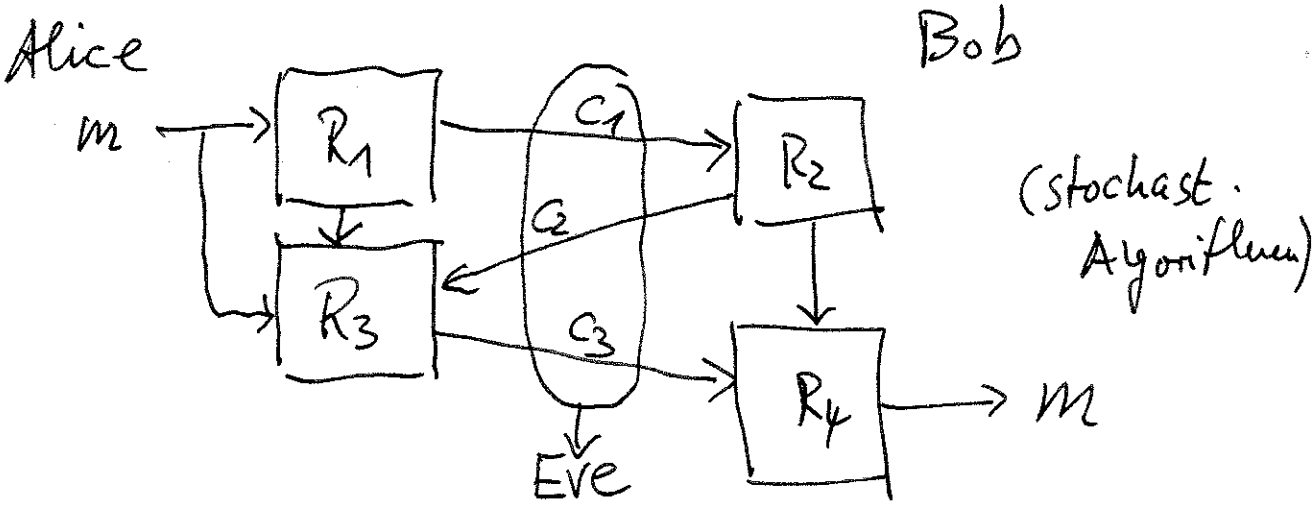
Weiteres:
Authentifizierung
Signatur
Zero knowledge
elektr. Münzen
elektr. Wahlen
Steganographie

Klassisches Szenario



Moderne Kryptographie (seit 1976)

- Diffie/Hellman: „New Directions in Crypto."



Runden-Algorithmen

Protokoll

Kerckhoff'sches Prinzip:
Ver/Entschlüsselungsalgorithmen sind bekannt. Sicherheit hängt von Verfahren und von Schlüssel(länge) ab

Historische Verfahren

Permutationschiffren:

F	M	E	E	E	S
O	H	T	A	N	N
I	R	G	M	G	E
R	M	E	D	E	N
R	F	A	E	U	R
X	F	I	R	F	U

Anzahl Schlüssel: 4^9

Substitutionschiffren (monoalphabetisch):

c: $A \mapsto D$, $B \mapsto E$, $C \mapsto F$, $\vdots$, $Z \mapsto C$

Cäsar-Chiffre, um 3 Buchstaben versetzt (kein Schlüssel)

Veralgemeinerung: $(A, B, \ldots, Z) \hat{=} (0, 1, \ldots, 25)$

$$E(a, k) = (a + k) \bmod 26 = c$$

- a: Klartext-Buchstabe
- k: Schlüssel, $k \in \{0, 1, \ldots, 25\}$
- c: Chiffre-Buchstabe

Affine Chiffre:

$$E(a, (k_1 k_2)) = (k_1 \cdot a + k_2) \bmod 26$$

k_1 muss teilerfremd zu 26 sein

$\varphi(26) = 12$ Anzahl Schlüssel: $12 \cdot 26 = 312$

Allgemeine monoalphabetische Codierung:

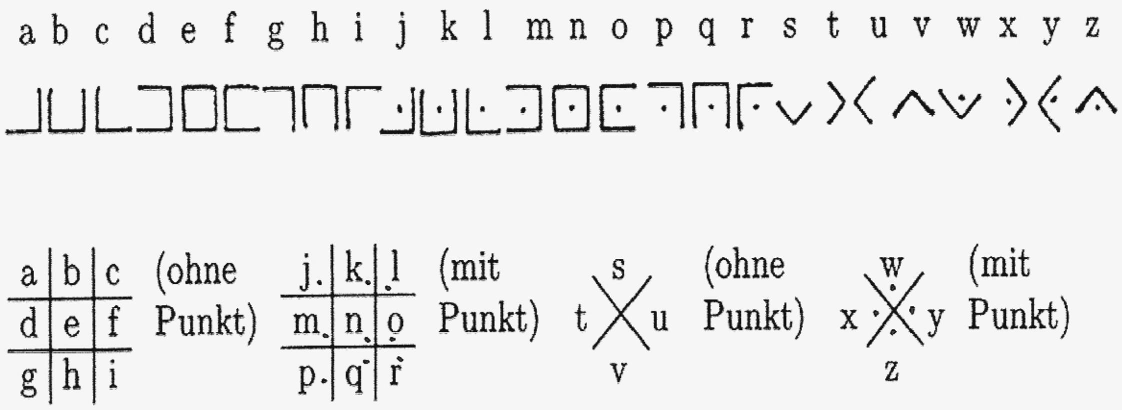
$$\pi: \begin{array}{l} A \mapsto F \\ B \mapsto Y \\ \vdots \\ Z \mapsto X \end{array}$$

Anzahl Schlüssel: $26! \approx 2^{88}$

Ausreichend große Zahl von Schlüsseln, trotzdem leicht zu knacken.

Bilder:

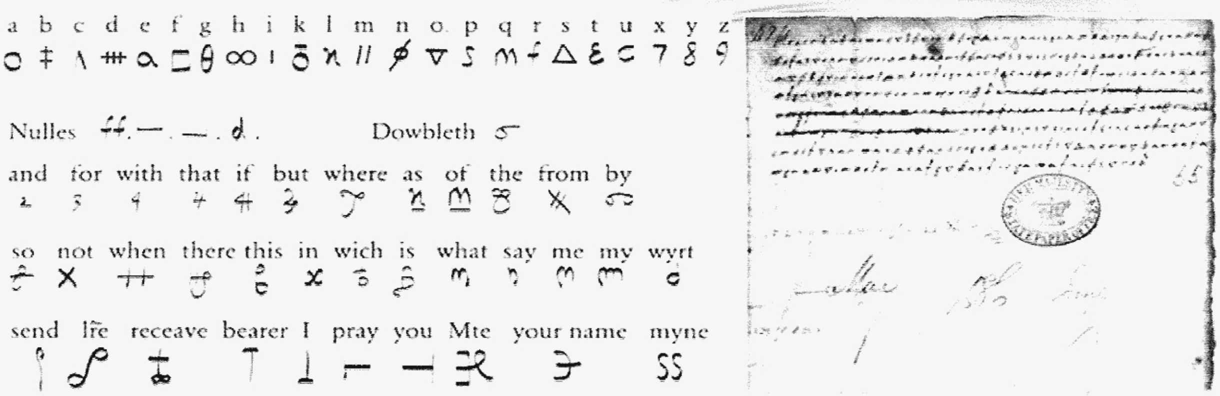
Die Freimaurer-Chiffren



Freimaurer-Chiffre mit speziellen Anordnungen als Merkhilfe (unten)

Die so genannte Freimaurer-Chiffre ist vermutlich ca. 1740 in Frankreich entstanden. Das Chiffrieralphabet besteht hier aus den untenstehend dargestellten 26 Symbolen.

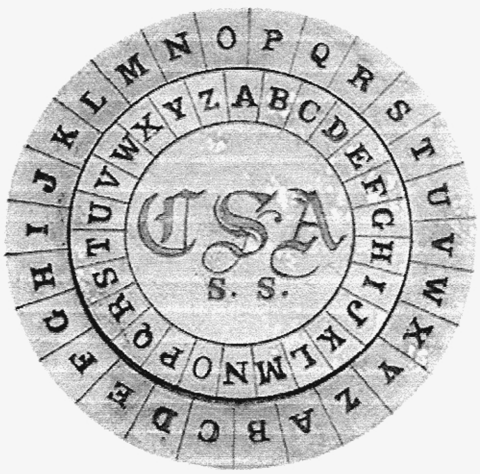
Maria Stuart (1542 – 1587)



Public Records Office, London

Maria Stuart wurde - aufgrund ihrer Korrespondenz und dem Nachweis des Codebuchs - wegen Hochverrats zum Tode verurteilt und am 8. Februar 1587 auf Fotheringhay Castle enthauptet.

Confederate Cipher Disk



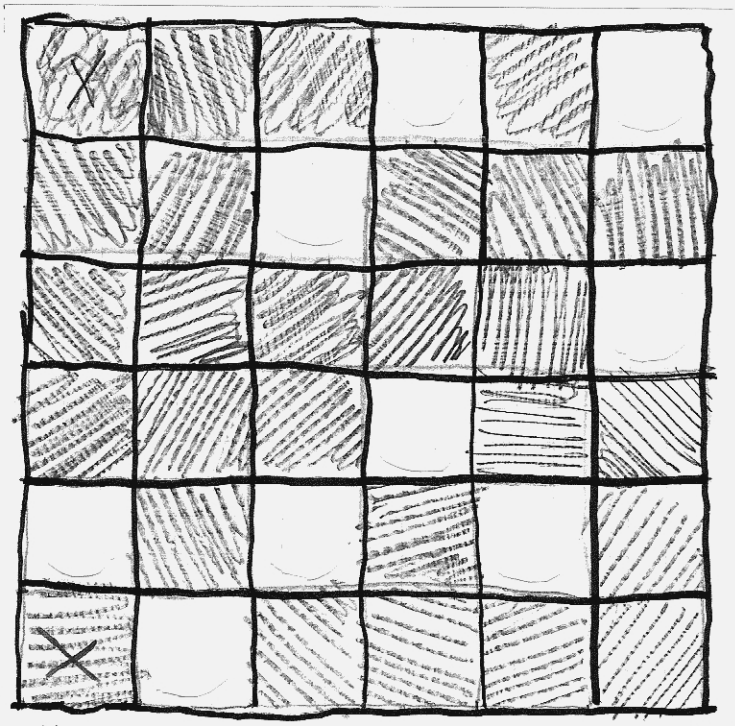
Diese Chiffrierscheibe aus Messing, die eine Substitutionsverschlüsselung realisiert, wurde vom Nachrichtendienst der Konföderierten im amerikanischen Sezessionskrieg der Nord- gegen die Südstaaten in den Jahren 1861 - 1865 eingesetzt.

In Königsberg i. Pr. gabelt sich der Pregel und umfließt eine Insel, die *Kneiphof* heißt. In den dreißiger Jahren des achtzehnten Jahrhunderts wurde das Problem gestellt, ob es wohl möglich wäre, in einem Spaziergang jede der sieben Königsberger Brücken genau einmal zu überschreiten.

Daß ein solcher Spaziergang unmöglich ist, war für L. EULER der Anlaß, mit seiner anno 1735 der Akademie der Wissenschaften in St. Petersburg vorgelegten Abhandlung *Solutio problematis ad geometriam situs pertinentis* (Commentarii Academiae Petropolitanae 8 (1741) 128-140) einen der ersten Beiträge zur Topologie zu liefern.

Das Problem besteht darin, im nachfolgend gezeichneten Graphen einen einfachen Kantenzug zu finden, der alle Kanten enthält. Dabei repräsentiert die Ecke vom Grad 5 den Kneiphof und die beiden Ecken vom Grad 2 die Krämerbrücke sowie die Grüne Brücke.

(Beispiel für Steganographie)



Buchstabenhäufigkeiten im Deutschen