Kryptologie Teil 1

Ziele

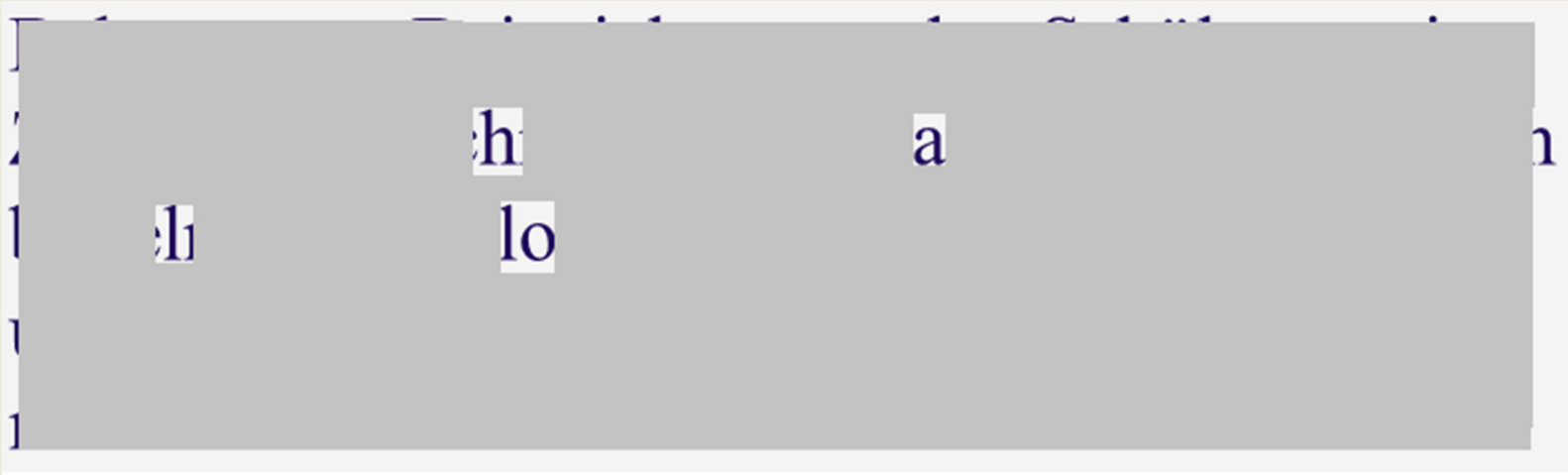
- Anhand historischer Verschlüsselungsverfahren Grundprinzipien der Kryptografie kennen lernen.
- Klassische Analysemethoden kennen lernen und sich dadurch der verbleibenden Restrisiken der Verschlüsselung bewusst werden.
- «Wettlauf» der Kryptographen und der Kryptoanalytiker «begreifen»

Abgrenzung gegen Steganographie

- Verstecken der Nachricht

- Bekannteste Beispiele unter den Schülern: mit Zitronensaft schreiben und das Papier zum Lesen bügeln. / Schablone und bekannten Text nutzen und durch die Schablone neuen Text sichtbar machen

Abgrenzung gegen Steganographie



Abgrenzung gegen Steganographie

- z.B. Urheber von Bildern, Filmen, Musik verstecken Informationen, um Missbrauch vorzubeugen

Das Problem

Nur Bob soll die Nachricht von Alice empfangen können…

Alice

Maloy (Schnüffler)

Bob

Mithören, Manipulieren

Klartext → Gleicher Klartext?

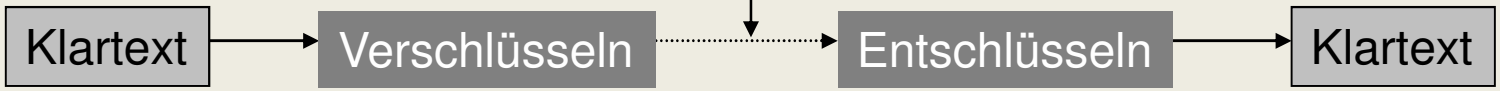
Die Lösung

Maloy (Schnüffler)

Alice

Bob

Kein Mithören, kein Manipulieren?



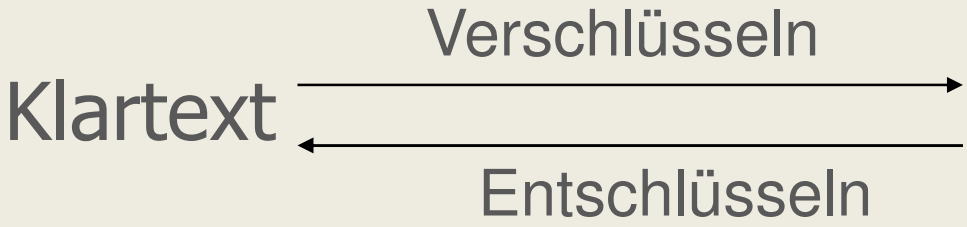
Übersicht

Kryptologie: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptografischen Verfahren

Kryptografie: Wie kann eine Nachricht ver- und entschlüsselt werden?

Kryptoanalyse: Wie sicher ist ein Ver-schlüsselungsverfahren?

Klassische Kryptografie



Der Klartext (K) wird mittels eines Schlüssels verschlüsselt.

Mit Hilfe desselben Schlüssels kann der Geheimtext (G) wieder entschlüsselt werden.

Geheime Übermittlung

- Voraussetzungen:
  - Der Empfänger kennt den Schlüssel.
  - Aber sonst niemand.
  - Ohne Kenntnis des Schlüssels ist es unmöglich oder sehr schwierig den Klartext herauszufinden.

- Schwierigkeiten:
  - Schlüssel muss vorher vereinbart werden.
  - Schlüssel muss geheim bleiben → „geheimer Kanal“.
  - Das Verschlüsselungsverfahren muss sicher sein.
  - Für jeden Kommunikationspartner eigenen Schlüssel

Das Caesar-Verfahren

- Julius Caesar (50 Jahre v. Chr.)
- Das Alphabet wird einfach um mehrere Buchstaben verschoben.
- Zum Beispiel um 3 Buchstaben:

abc**defghijklmnopqrstuvwxyz**
DEFGHIJKLMNOPQRSTUVWXYZABC

- Damit wird aus dem Klartext „hallo“ der Geheimtext „KDOOR“.

Entschlüsselung

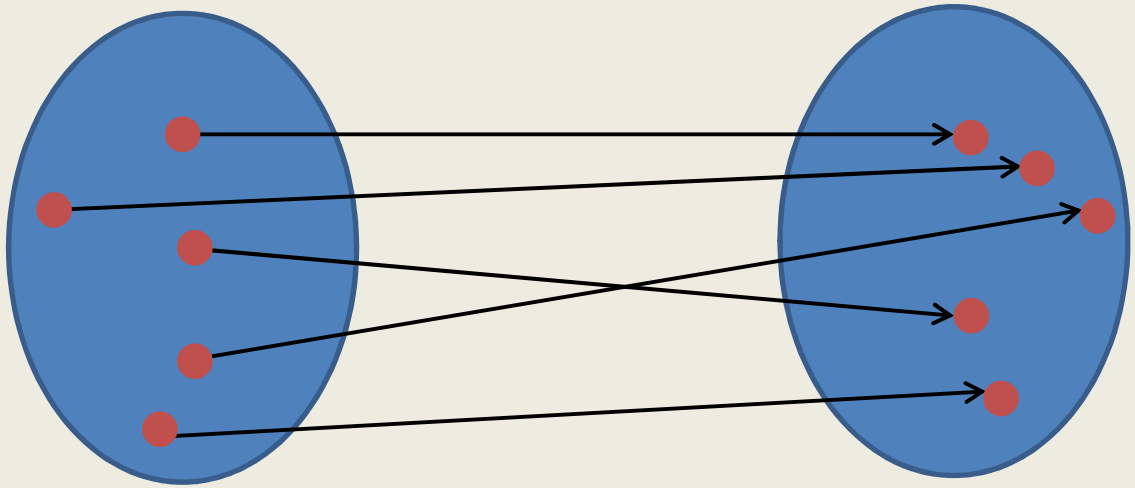
- Die Entschlüsselung ist die Umkehrung der Verschlüsselung
- Das heisst beim Beispiel-Caesar-Verfahren jetzt um 3 Buchstaben zurückverschieben:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
xyzabcdefghijklmnopqrstuvw
```

- So wird aus „KDOOR“ wieder ein „hallo“.
- Der Schlüssel ist eine Zahl zwischen 1 und 25 (26)

Monoalphabetische Verfahren

- Die Caesar-Verschlüsselung ist ein monoalphabetisches Verfahren
  → Aus einem bestimmten Klartextbuchstaben wird immer *derselbe* Geheimtextbuchstabe.



Menge der Klartextzeichen

Menge der Geheimtextzeichen

Allgemeine Substitutionsverfahren

Als Verallgemeinerung der Caesar-Verschiebung

Substitutionsverfahren

- Bei dem Substitutionsverfahren wird jedem Buchstaben ein beliebiges anderes Symbol (eventuell ein anderer Buchstabe) zugeordnet.
- Allerdings muss diese Zuordnung eindeutig sein

- Anm.: Dies ist meist die erstgenannte Verschlüsselung der Schüler, wenn man sie nach ihren Vorstellungen fragt.
- Fehlvorstellung: Je „komplizierter“ die Ersetzungen, desto sicherer ist die Verschlüsselung!

Beispiel

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
1	Z	!	@	3	X	€	W	5	V	6	?	7	T	8	S	9	%	(	Q	)	P	=	N	+	M

Damit wird aus dem Klartext „HALLO“ der Geheimtext „W1??8“.
Aus dem „L“ wird beide Male ein „?“

⇒ monoalphabetisch

Entschlüsseln Sie den Satz:
T5!WQ V3@3(S%8Z?37 5(Q ?83(Z1%

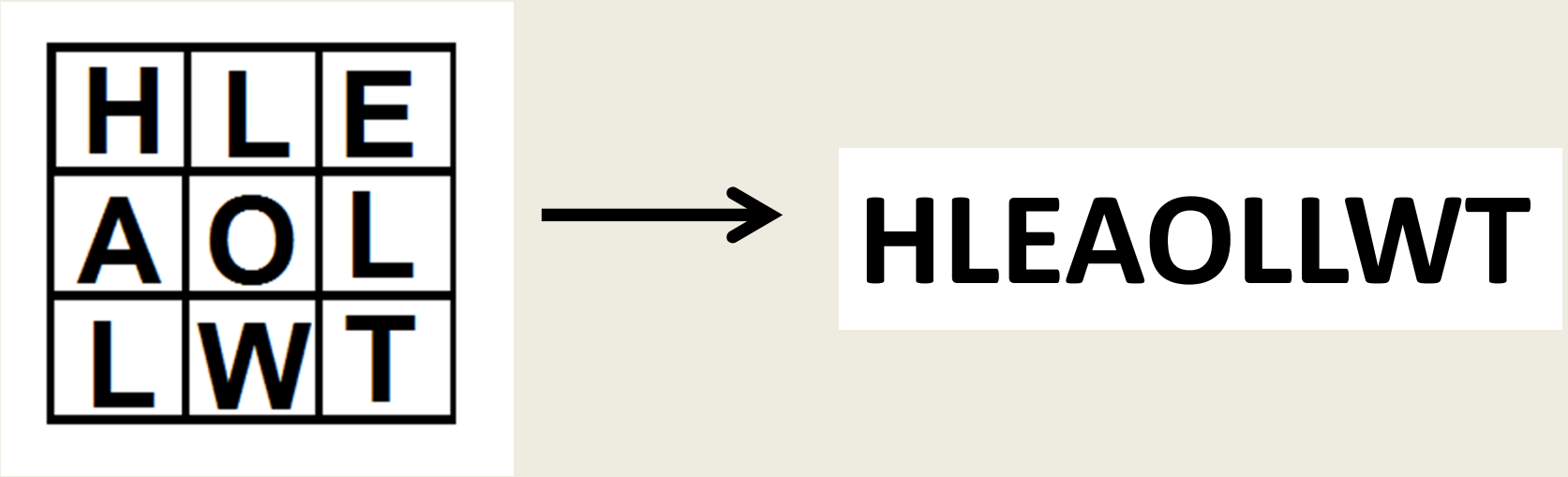
Transposition

- Skytale http://commons.wikimedia.org/wiki/File:Skytale.png, Zugriff: 13.8.2012

- Programmierbeispiel in Java:
  - zweidimensionale Reihung: Text spaltenweise eingeben und zeilenweise auslesen

Transposition

- Programmierbeispiel in Java:
  - zweidimensionale Reihung: Text spaltenweise eingeben und zeilenweise auslesen
  - Schlüssel ist die Größe des Feldes

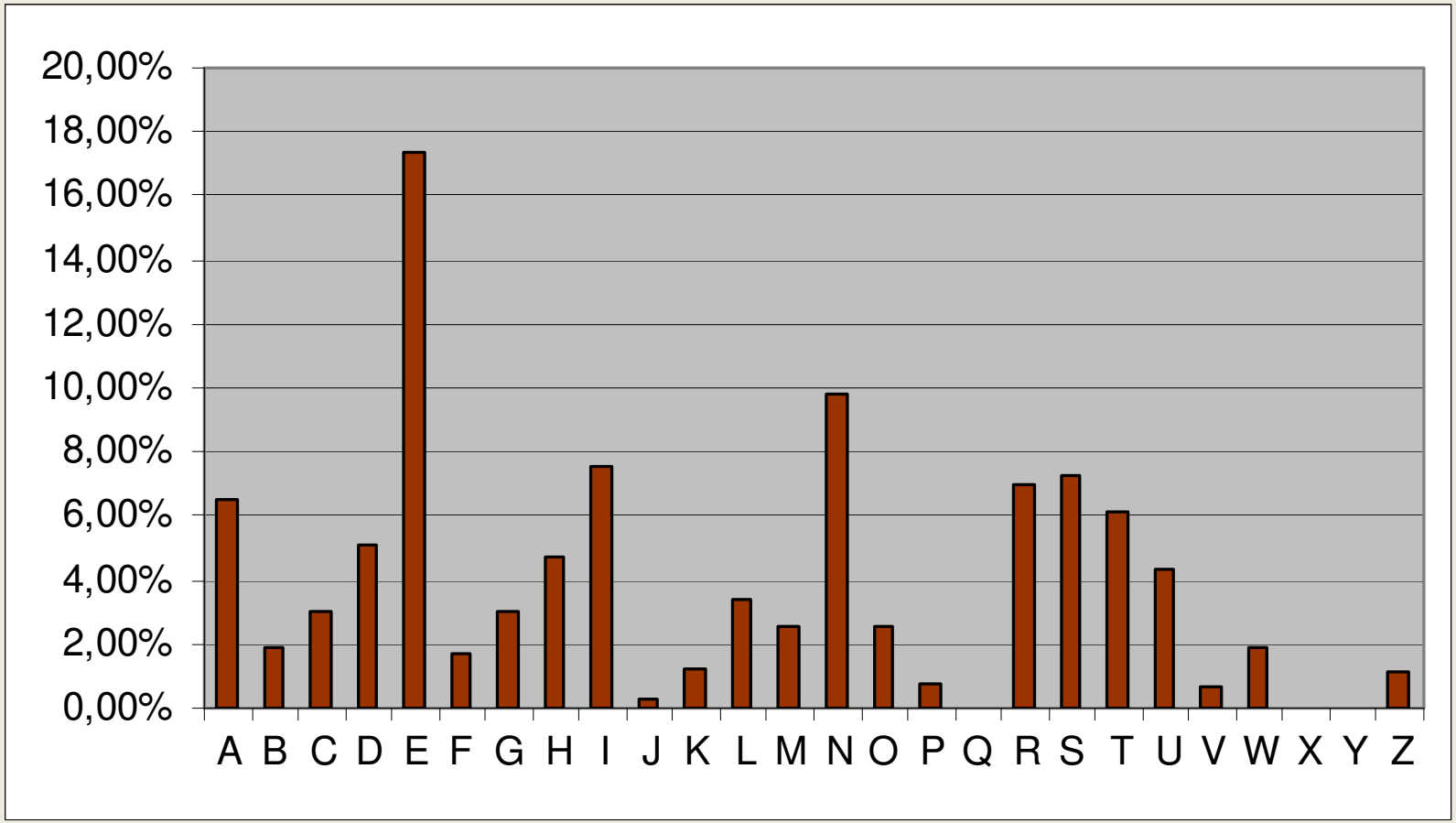


Die Entschlüsselung monoalphabetischer Verfahren

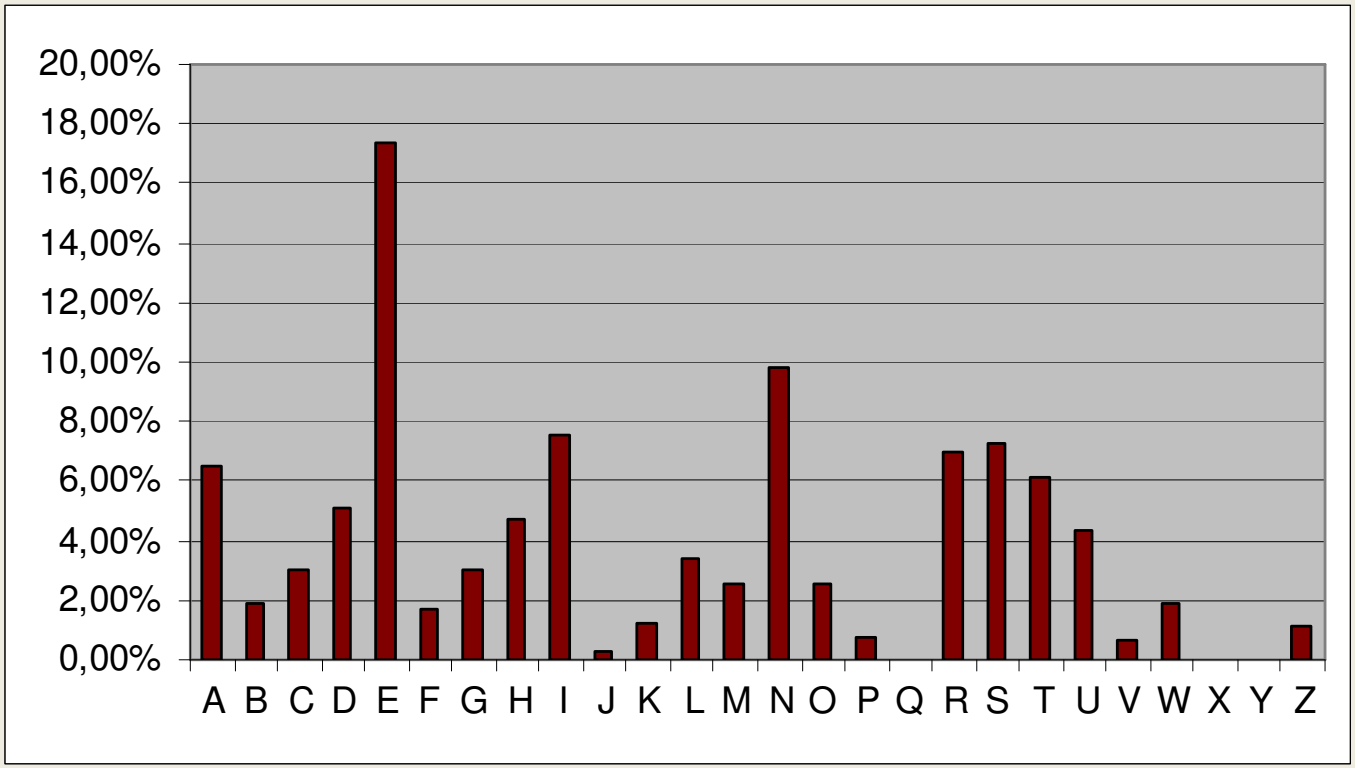
Entschlüsslung monoalphabetischer Verfahren

- Erstmals beschrieben im 9. Jh in der arabischen Welt
- beruht auf unterschiedlichen Häufigkeiten eines Buchstabens in einer Sprache

Häufigkeitsverteilung der Buchstaben des deutschen Alphabets



Entschlüsselung



W?WW?W 1@? ?@W 2?@1(@?)

Häufigkeitsanalyse

- den Geheimtext betrachten
- die einzelnen Symbole nach Häufigkeit sortieren
- vergleichen mit den Häufigkeiten des Klartextalphabets
- sinnvolle Schlüsse ziehen (keine allzu schablonenhafte Anwendung)
- Nach Häufungen bestimmter Wörter oder Buchstabenkombinationen suchen
- Symbole durch Buchstaben ersetzen

Grenzen der Häufigkeitsanalyse

- der verschlüsselte Text muss hinreichend lang sein
- die Sprache des Klartextes muss bekannt sein
- Achtung bei Texten mit ungewöhnlichen Worthäufungen („Taxitext“)
- Oft sind logische Überlegungen

Schlussfolgerung

- *Monoalphabetische* Verschlüsselungsverfahren können mit der Häufigkeitsanalyse „geknackt“ werden.

Übung

- Wenn man die Häufigkeitsanalyse auf Caesar-verschlüsselte Texte anwendet vereinfacht sie sich insofern, als dass man nur das „e“ identifizieren muss. Warum?
- Entschlüsseln Sie den mit Caesar verschlüsselten Satz: „LIYXI IWWI MGL IMR IMW“ ohne Kenntnis des Schlüssels.
- Bilden Sie einen Satz mit mindestens 10 Wörtern ohne ein einziges „e“.
- Entschlüsseln Sie in Word den Geheimtext
- Sammeln Sie Informationen über die „Beale-Chiffren“

Übung

„Knacken“ Sie mit der Häufigkeitsanalyse den Geheimtext, der als Word-Dokument vorliegt. Gehen Sie folgendermaßen vor:

Unter dem Menüpunkt „Bearbeiten“ wählen Sie „Ersetzen“ und ersetzen ein Geheimbuchstaben zunächst durch sich selbst, also z.B. ein „S“ durch ein „S“. Der Text verändert sich nicht, Word gibt aber an, wie viele Ersetzungen vorgenommen wurden (1.066). So können Sie die Häufigkeiten der einzelnen Zeichen erfassen. Jetzt stellen Sie fest, dass kein anderer Buchstabe so oft vorkommt und schließen daraus, dass es sich bei dem „S“ um das Klartext-“e“ handelt. Dies ersetzten Sie nun, nachdem Sie (**wichtig!**) „Groß- und Kleinschreibung unterscheiden“ angeklickt haben. Alle Klartextbuchstaben, die nicht verschlüsselt wurden wie Satzzeichen, Umlaute oder das „ß“ sind bereits klein geschrieben.