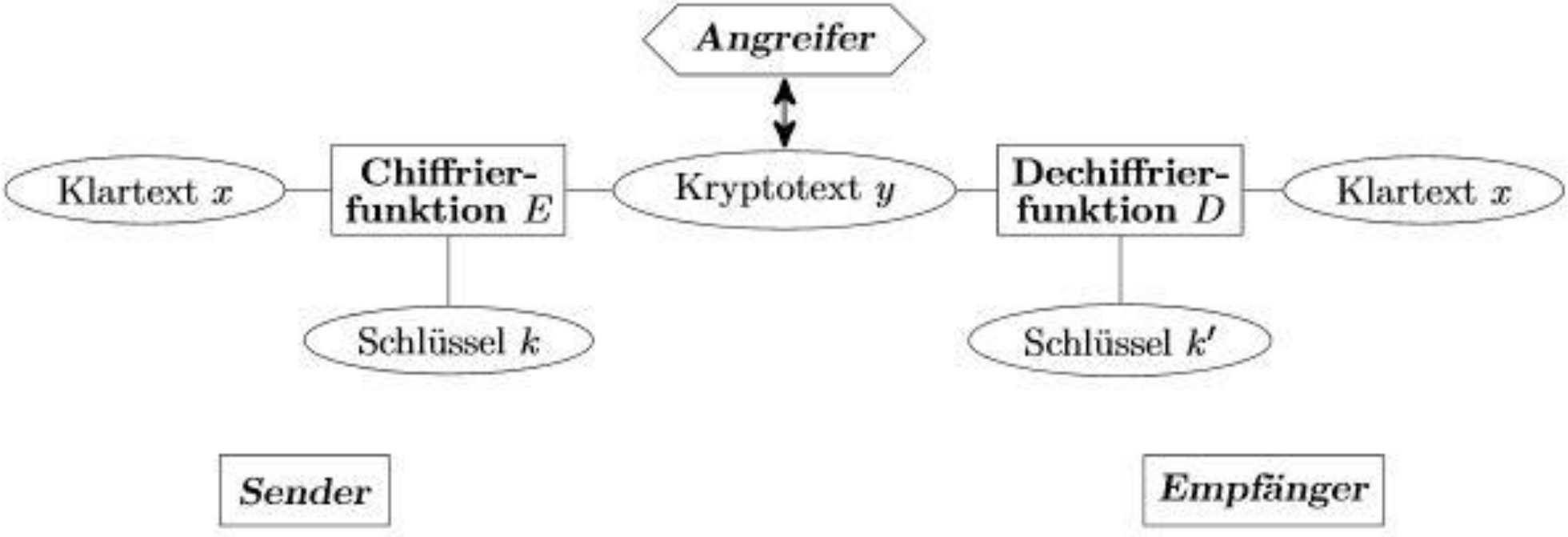
Cryptool 2 - Kryptoanalyse

Dominic Bublitz

Einleitung

- Kryptographie wird benutzt, um Informationen zu schützen
- In der Antike wurden Informationen bereits verschlüsselt
- Methoden wurden über die Zeit immer komplexer
- Beispiele:
  - Caesar Verschlüsselung
  - Skytale (antikes Griechenland)
  - ENIGMA
  - AES
  - …

Allgemeine Kommunikation



Kryptographie

- Klartext x wird mit der Chiffrierfunktion E unter der Verwendung des Schlüssels k verschlüsselt
- Chiffrierfunktion kann beliebig komplex sein und auch bekannt
- Schlüssel muss geheim sein!

Der Schlüssel muss geheim gehalten werden, aber nicht der Verschlüsselungsalgorithmus

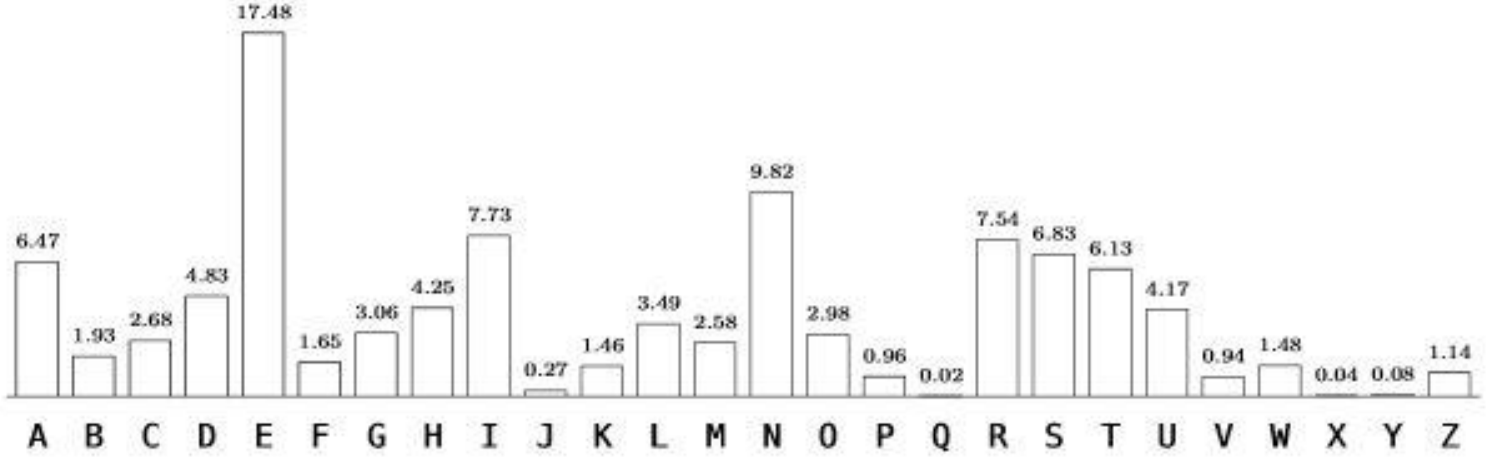
Kerckhoffs‘ Prinzip

Methoden der Kryptoanalyse

1. Brute-Force Angriff
   - Generiert alle möglichen Schlüssel und probiert diese aus
   - Sehr ineffizient, da im worstcase alle Schlüssel ausprobiert werden
2. Wörterbuch Angriff
   - Alle Schlüssel aus einer vordefinierten Liste werden probiert
   - Schlüssel kann nicht in der Liste vorhanden sein, daher höhere Wahrscheinlichkeit für einen Fehlschlag

Statistische Analyse

- Analyse von Häufigkeiten (Zeichen, Kombinationen von Zeichen)
- Jede Sprache hat seine eigenen Besonderheiten an Häufigkeiten
- Häufigkeitsverteilung in der deutschen Sprache:



Statistische Analyse

- Findet seinen Einsatz z.B. bei Substitutionschiffren (Caesar, Vigenère)
- Problem bei Stromchiffren ist, dass der Schlüssel immer angehangen wird und so Zeichen sich verändern.
- Beispiel:
  - Klartext: dertest Schlüssel: key
  - (dertest) + (keykeyk) = OJPEJQE

Statistische Analyse

- Zu erst muss die Länge des Schlüssel bestimmt werden:

1. Der Kasiski Test:
   - Ermittelt den Abstand gleich langer Folgen
   - Länge des Schlüssels ist entweder der Abstand selbst oder ein Teil seiner Primfaktorzerlegung
2. Friedmann Test
   - Kann die Ergebnisse des Kasiski Tests bestätigen
   - Berechnet die Wahrscheinlichkeit, wie hoch die Wahrscheinlichkeit ist, dass an zwei zufälligen Positionen der gleiche Buchstabe steht

Statistische Analyse

- Dieser Index heißt Koinzedenzindex (IC) $\mathrm{IC} = \frac{\sum_{i=A}^{Z} n_i(n_i - 1)}{N(N-1)}$
- Die Summe im Zähler berechnet das Vorkommen jedes Zeichens (n) aus dem Alphabet (A-Z)
- Im Nenner steht N für die Gesamtzahl der Zeichen im Text

- Die Länge des Schlüsselwortes ergibt folgende Formel

Statistische Analyse

- 0,0762 ist die Häufigkeit für die deutsche Sprache, 0,0385 ist das absolute Minimum für den IC
- n ist die Anzahl der Zeichen

$$l = \frac{(0{,}0762 - \frac{1}{26})n}{IC * (n-1) - 0{,}0385n + 0{,}0762}$$

- Nach Bestimmung der Länge kann die einfache Häufigkeitsanalyse vorgenommen werden

Cryptool 2

Cryptool 2

- Bietet praktische Möglichkeiten Verschlüsselungen und kryptoanalytische Methoden auszuprobieren
- Lehrprogramm entwickelt u.a. von der Uni-Siegen
- Open-Source Programm aktuell in der Betaphase

Live Demo

Vigenère-Quadrat

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