Anwendungen der Linearen Algebra: Kryptologie

Philip Herrmann

Universität Hamburg

5.12.2012

„No one has yet discovered any warlike purpose to be served by the theory of numbers (...)“, G.H.Hardy, A Mathematician's Apology, 1940.

Was ist Kryptologie?

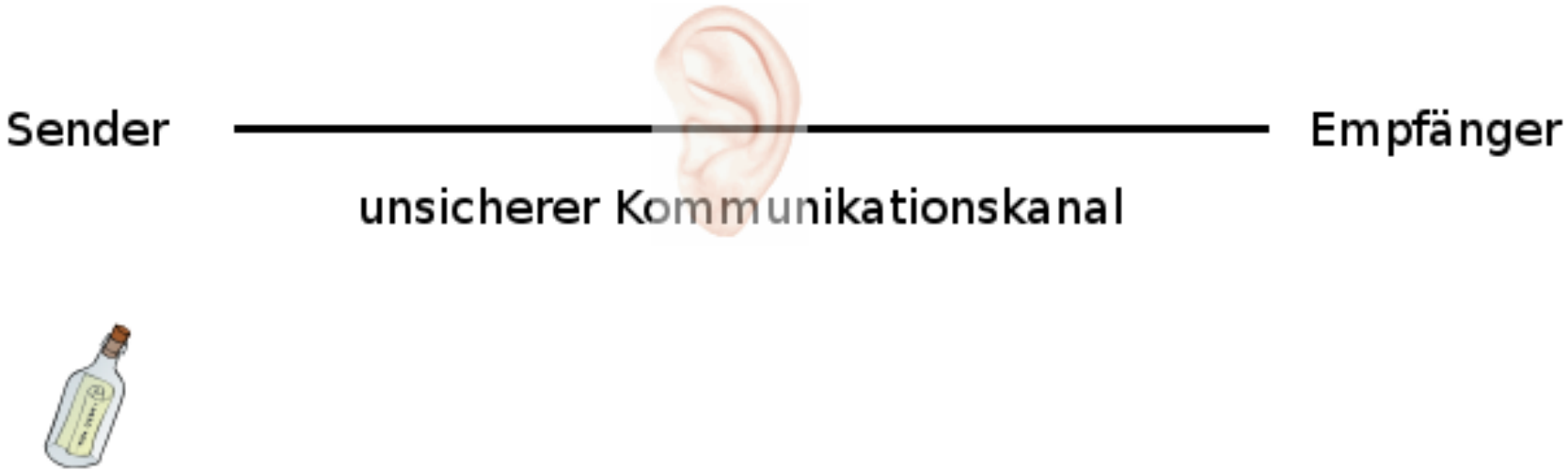
- Kryptós - Geheim, Verborgen

Was ist Kryptologie?

- Kryptós - Geheim, Verborgen
- Kryptographie – Ver- und Entschlüsselung von Nachrichten
- Kryptoanalyse – Theorie der Angriffe auf verschlüsselte Nachrichten

Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

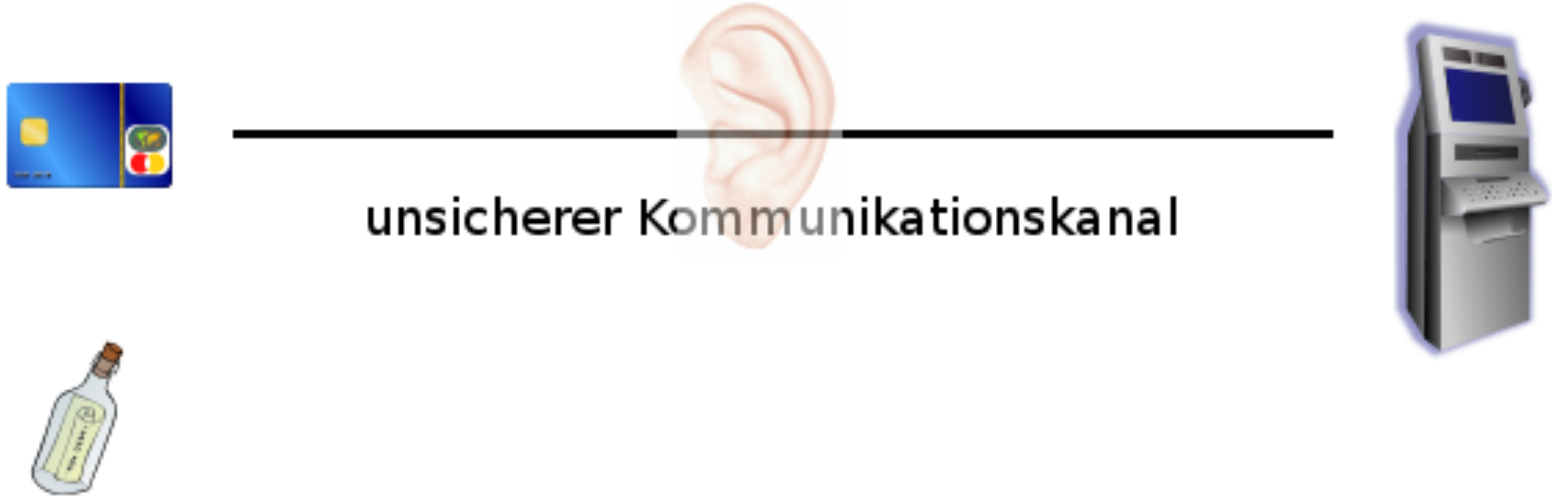


Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

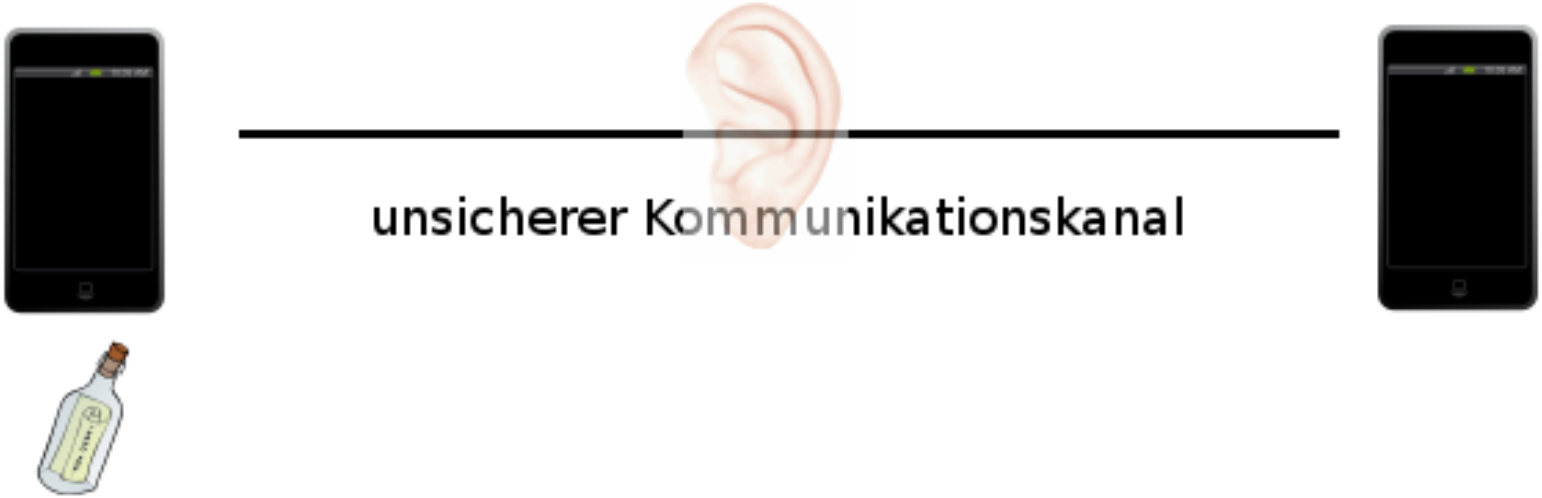
Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?



Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?



Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

unsicherer Kommunikationskanal

Alice

Bob

Ein Kommunikationsmodell

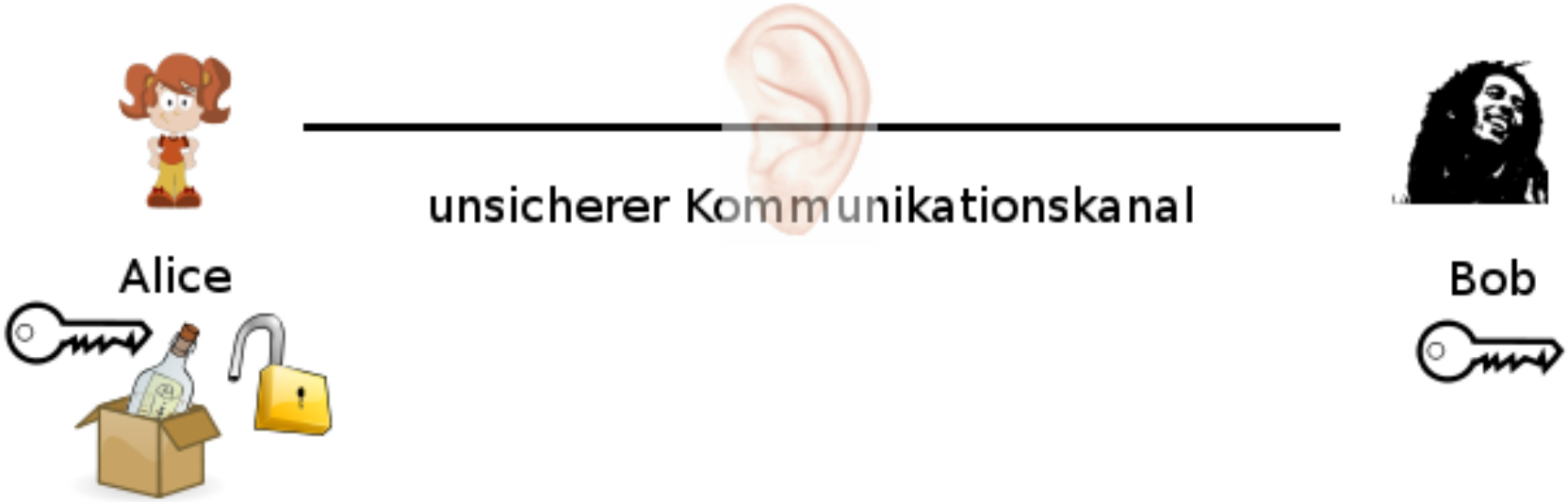
Vertrauliche Kommunikation über einen unsicheren Kanal?

Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

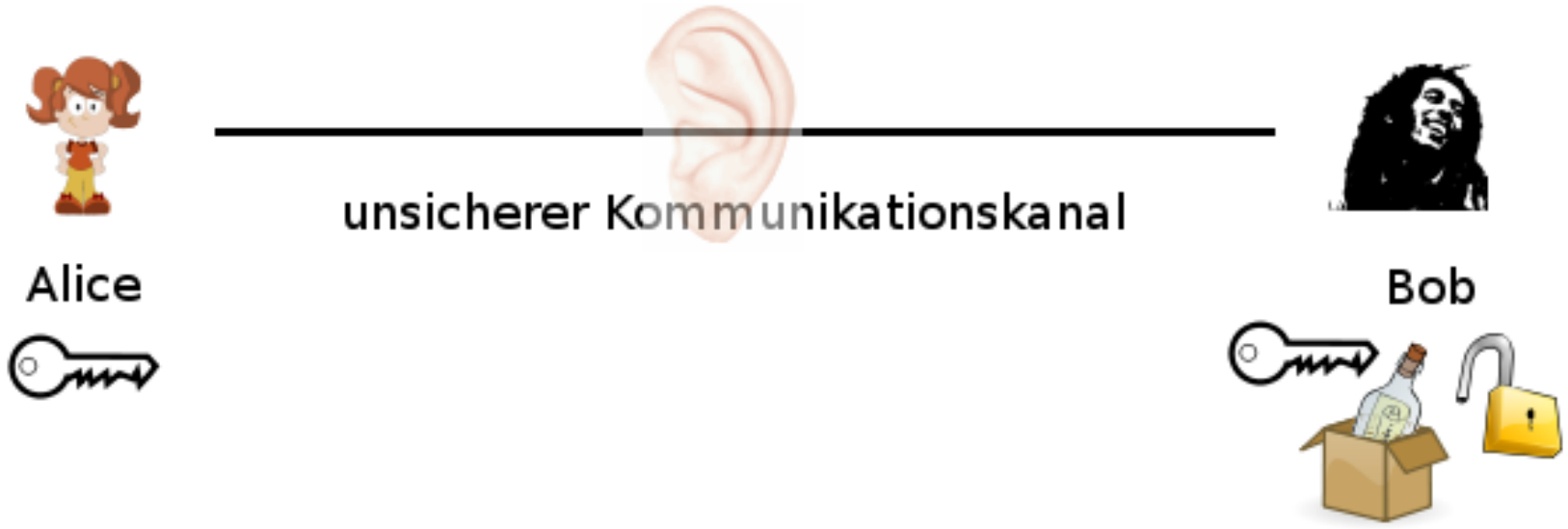


Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?

Ein Kommunikationsmodell

Vertrauliche Kommunikation über einen unsicheren Kanal?



Lösung: Verschlüsselung

Vertrauliche Kommunikation über einen unsicheren Kanal?

- Alice und Bob vereinbaren vorab ein gemeinsames Geheimnis $k \in K$!
- Alice und Bob vereinbaren ein Verfahren (E, D) um Nachrichten $m \in M$ mittels E so zu verschleiern, dass sie durch D nur mit Wissen von k lesbar sind

Lösung: Verschlüsselung

Vertrauliche Kommunikation über einen unsicheren Kanal?

- Alice und Bob vereinbaren vorab ein gemeinsames Geheimnis $k \in K$!
- Alice und Bob vereinbaren ein Verfahren (E, D) um Nachrichten $m \in M$ mittels E so zu verschleiern, dass sie durch D nur mit Wissen von k lesbar sind, also

$$E : M \times K \to C \tag{1}$$

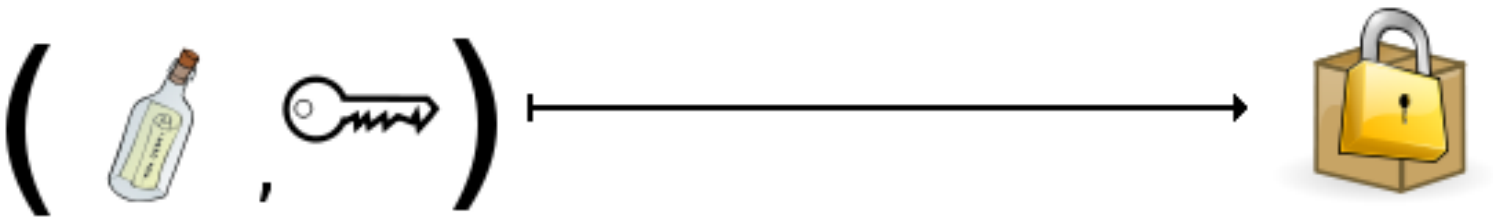
$$D : C \times K \to M \quad , \text{ so dass} \tag{2}$$

$$D(E(m,k),k') = \begin{cases} m & , \text{falls } k = k' \\ m' \neq m & , \text{falls } k \neq k'. \end{cases}$$

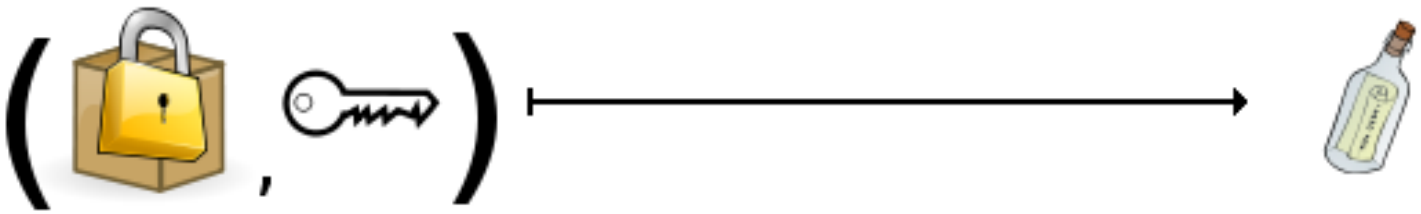
Lösung: Verschlüsselung

Vertrauliche Kommunikation über einen unsicheren Kanal?

$$E : M \times K \to C$$



$$D : C \times K \to M$$



Beispiel: Caesar-Chiffre

- $M = \{A, B, C, \ldots, Z\}$
- Verschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach rechts'.
- Entschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach links'.

Beispiel: $k = 3$

$$
\begin{aligned}
A &\rightsquigarrow D \\
B &\rightsquigarrow E \\
C &\rightsquigarrow F \\
&\vdots \\
W &\rightsquigarrow Z \\
X &\rightsquigarrow A \\
&\vdots \\
Z &\rightsquigarrow C
\end{aligned}
$$

Beispiel: Caesar-Chiffre

- $M = \{A, B, C, \ldots, Z\}$
- Verschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach rechts'.
- Entschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach links'.

Beispiel: $k = 3$

$A \rightsquigarrow D$
$B \rightsquigarrow E$
$C \rightsquigarrow F$
$\vdots$
$W \rightsquigarrow Z$
$X \rightsquigarrow A$
$\vdots$
$Z \rightsquigarrow C$

HERZLICH WILLKOMMEN ZU DIESEM VORTRAG UEBER EINE ANWENDUNG VON INHALTEN AUS DER VORLESUNG LINEARE ALGEBRA.

Beispiel: Caesar-Chiffre

- $M = \{A, B, C, \ldots, Z\}$
- Verschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach rechts'.
- Entschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach links'.

Beispiel: $k = 3$

A$\rightsquigarrow$ D	
B$\rightsquigarrow$ E	HERZLICH WILLKOMMEN ZU DIESEM VORTRAG
C$\rightsquigarrow$ F	UEBER EINE ANWENDUNG VON INHALTEN AUS
$\vdots$	DER VORLESUNG LINEARE ALGEBRA.
W$\rightsquigarrow$ Z	K
X$\rightsquigarrow$ A	
$\vdots$	
Z$\rightsquigarrow$ C	

Beispiel: Caesar-Chiffre

- $M = \{A, B, C, \ldots, Z\}$
- Verschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach rechts'.
- Entschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach links'.

Beispiel: $k = 3$

A$\rightsquigarrow$ D	
B$\rightsquigarrow$ E	HERZLICH WILLKOMMEN ZU DIESEM VORTRAG
C$\rightsquigarrow$ F	UEBER EINE ANWENDUNG VON INHALTEN AUS
$\vdots$	DER VORLESUNG LINEARE ALGEBRA.
W$\rightsquigarrow$ Z	KH
X$\rightsquigarrow$ A	
$\vdots$	
Z$\rightsquigarrow$ C	

Beispiel: Caesar-Chiffre

- $M = \{A, B, C, \ldots, Z\}$
- Verschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach rechts'.
- Entschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach links'.

Beispiel: $k = 3$

A$\rightsquigarrow$ D	
B$\rightsquigarrow$ E	HERZLICH WILLKOMMEN ZU DIESEM VORTRAG
C$\rightsquigarrow$ F	UEBER EINE ANWENDUNG VON INHALTEN AUS
$\vdots$	DER VORLESUNG LINEARE ALGEBRA.
W$\rightsquigarrow$ Z	KHU
X$\rightsquigarrow$ A	
$\vdots$	
Z$\rightsquigarrow$ C	

Beispiel: Caesar-Chiffre

- $M = \{A, B, C, \ldots, Z\}$
- Verschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach rechts'.
- Entschlüsseln: Verschiebe jeden Buchstaben um k Stellen 'nach links'.

Beispiel: $k = 3$

A$\rightsquigarrow$ D	
B$\rightsquigarrow$ E	HERZLICH WILLKOMMEN ZU DIESEM VORTRAG
C$\rightsquigarrow$ F	UEBER EINE ANWENDUNG VON INHALTEN AUS
$\vdots$	DER VORLESUNG LINEARE ALGEBRA.
W$\rightsquigarrow$ Z	KHUCOLFK ZLOONRPPHQ CX GLHVHP YRUWUDJ
X$\rightsquigarrow$ A	XHEHU HLQH DQZHQGXQJ YRQ LQKDOWHQ DXV
$\vdots$	GHU YRUOHVXQJ OLQHDUH DOJHEUD.
Z$\rightsquigarrow$ C	

Histogramme

Eine Schwachstelle der Caesar-Chiffren

Kerckhoffs'sches Prinzip

Die Sicherheit des Kryptosystems (E, D) darf nicht abhängig davon sein, dass (E, D) geheim gehalten wird.

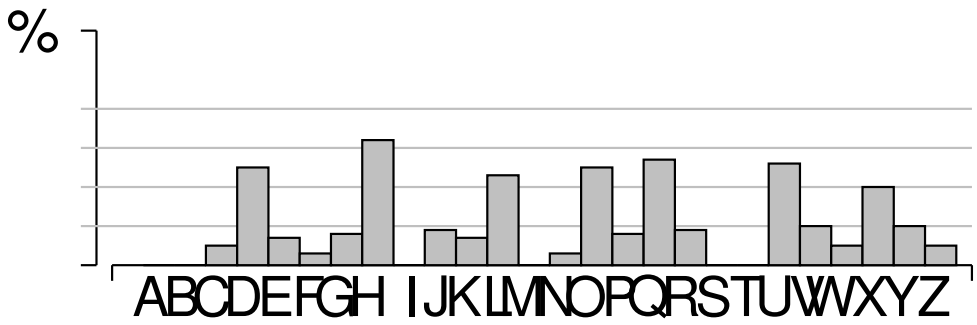
Problem: Bei Chiffren vom Typ der Caesar-Chiffre (monoalphabetische Subsitutionschiffren) spiegelen die Häufigkeiten der Schlüsseltextbuchstaben Informationen über die Häufigkeiten der Klartextbuchstaben wider.

Histogramme

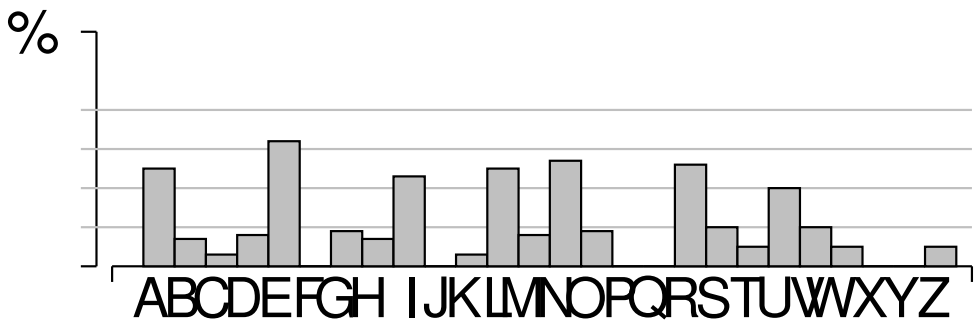
Eine Schwachstelle der Caesar-Chiffren

Häufigkeitsverteilung der Buchstaben:

Chiffrat:



Klartext:

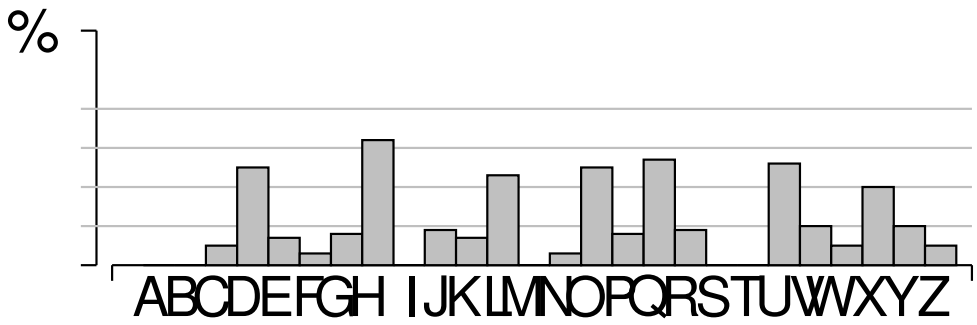


Histogramme

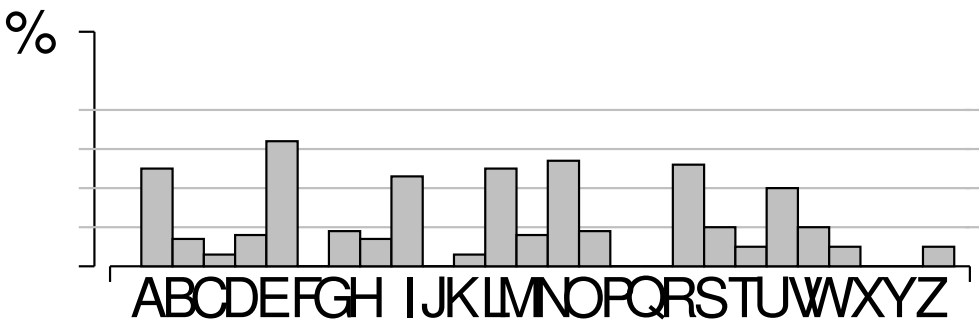
Eine Schwachstelle der Caesar-Chiffren

Häufigkeitsverteilung der Buchstaben:

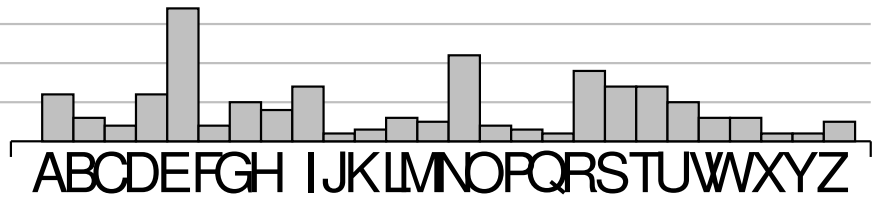
Chiffrat:



Klartext:

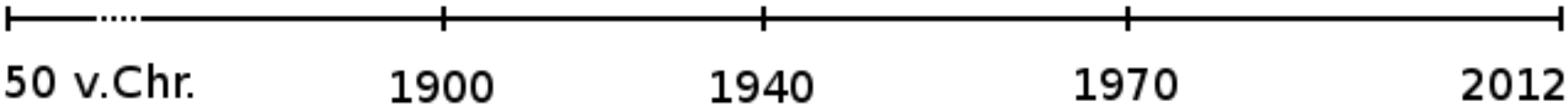


Deutsch:



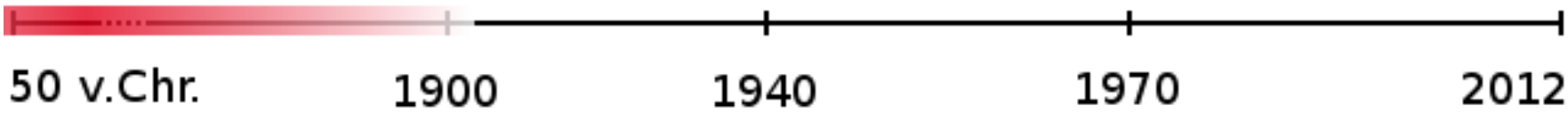
Geschichte der Kryptologie

Ein kurzer historischer Überblick



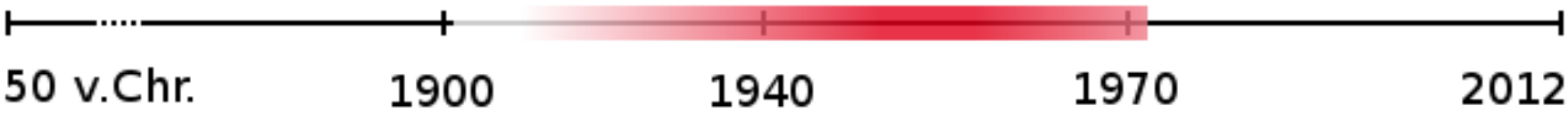
Geschichte der Kryptologie

Ein kurzer historischer Überblick



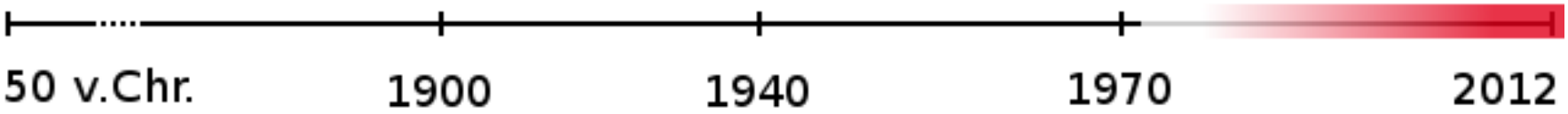
Geschichte der Kryptologie

Ein kurzer historischer Überblick



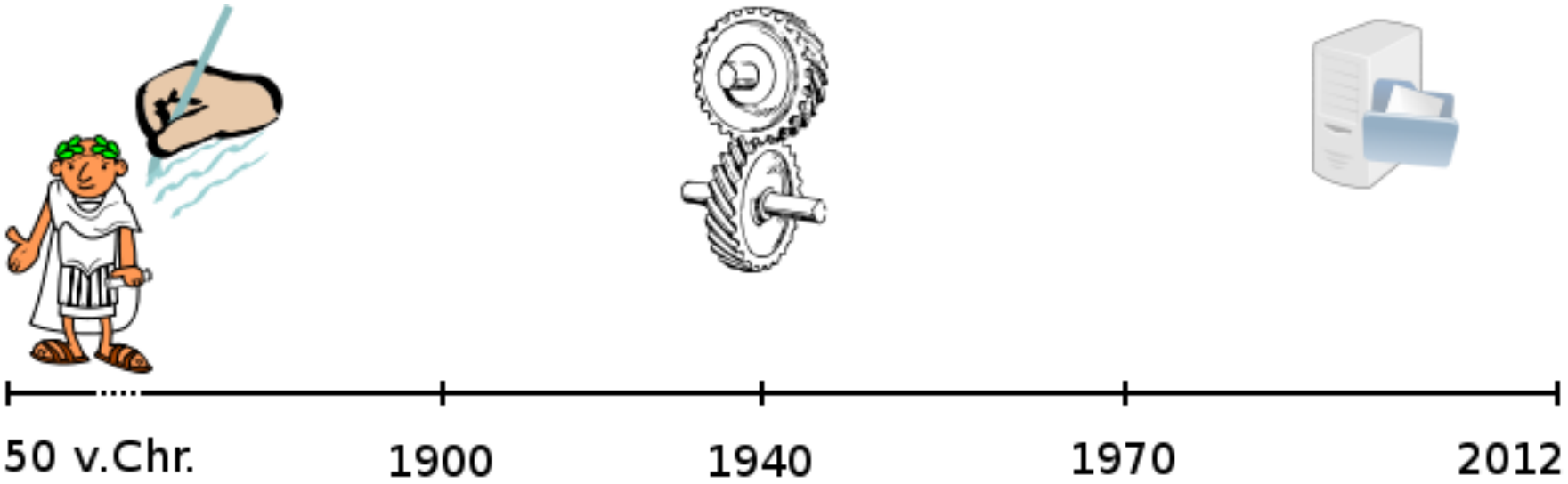
Geschichte der Kryptologie

Ein kurzer historischer Überblick



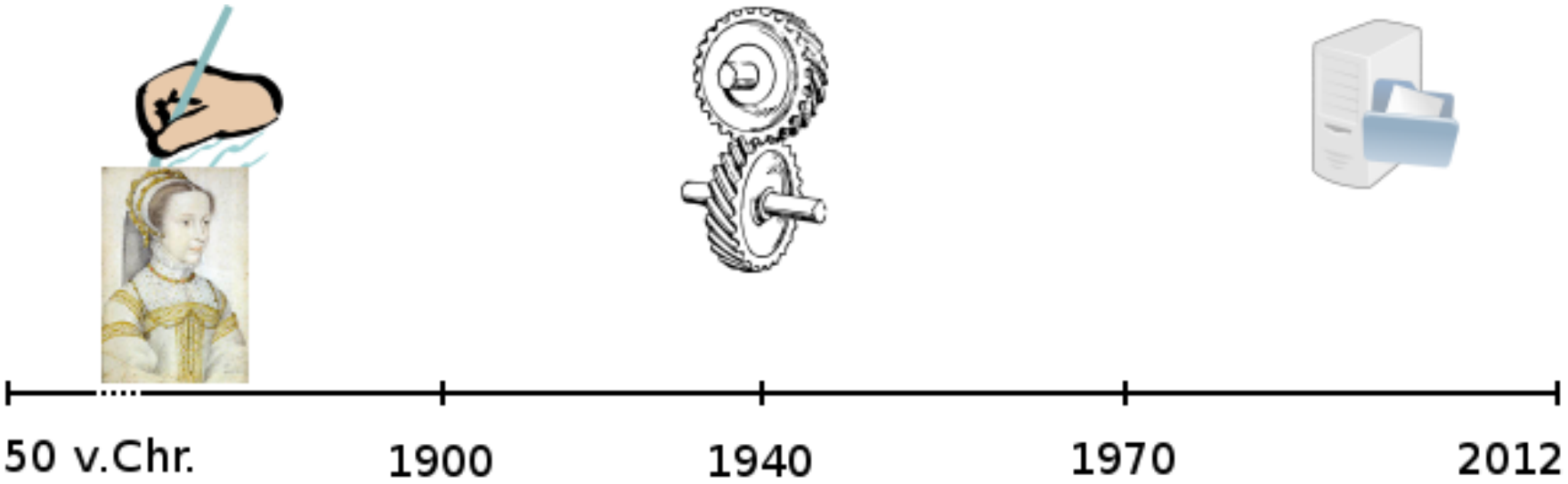
Geschichte der Kryptologie

Ein kurzer historischer Überblick



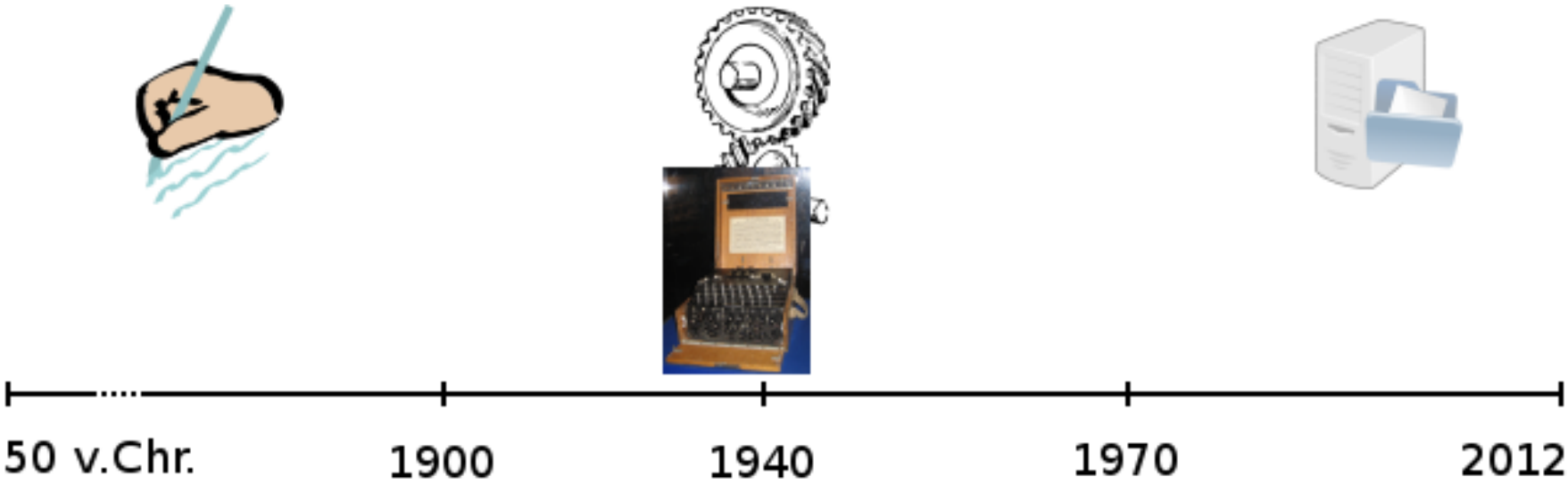
Geschichte der Kryptologie

Ein kurzer historischer Überblick



Geschichte der Kryptologie

Ein kurzer historischer Überblick



Geschichte der Kryptologie

Ein kurzer historischer Überblick

RSA

ECC

DES

AES

50 v.Chr. 1900 1940 1970 2012

Der RSA-Algorithmus

Ein paar Worte zu asymmetrischer Verschlüsselung

Frage

Muss man vor der geheimen Kommunikation schon ein Geheimnis k austauschen?

Idee

Bob ersetzt $E : M \times K \to C$ durch eine Funktion $E : M \to C$, für die nur Bob (in angemessener Zeit) Urbilder errechnen kann.

Der RSA-Algorithmus

Mathematische Türfallen

- Einwegfunktion

$$E : M \hookrightarrow C,$$

so dass

- $E(m)$ 'leicht' zu berechnen ist, aber
- $E^{-1}(c)$ 'sehr schwer' zu berechnen ist.

Der RSA-Algorithmus

Mathematische Türfallen

- Einwegfunktion mit Falltür

$$E : M \hookrightarrow C,$$

so dass

- $E(m)$ 'leicht' zu berechnen ist, aber
- $E^{-1}(c)$ 'sehr schwer' zu berechnen ist.
- Mit Extrawissen ist allerdings $E^{-1}(c)$ 'einfach' zu berechnen.

Der RSA-Algorithmus

Mathematische Türfallen

- Einwegfunktion mit Falltür

$$E : M \hookrightarrow C,$$

so dass

- $E(m)$ 'leicht' zu berechnen ist, aber
- $E^{-1}(c)$ 'sehr schwer' zu berechnen ist.
- Mit Extrawissen ist allerdings $E^{-1}(c)$ 'einfach' zu berechnen.

Beispiele: $g \mapsto g^n$ oder $n \mapsto g^n$ für bestimmte Kombinationen von n, g, G.

Der RSA-Algorithmus

- Der RSA-Algorithmus benutzt das diskrete Wurzelproblem ('RSA-Problem') $g \mapsto g^n$.
- Benannt nach Rivest, Shamir, Adleman, die den Algorithmus 1977 publizierten.
- Möglicherweise schon 1973 von Clifford Cocks erfunden.
- Gilt als sehr sicher, ist aber höchstens solange sicher, wie Primfaktorzerlegung ein schwieriges Problem ist.

Der RSA-Algorithmus

1. Nehme zwei Primzahlen große p, q und setze $n = p \cdot q$.
2. Wähle beliebiges $e \in \{2, \ldots, n-1\}$, mit $\mathrm{ggT}(e, n) = 1$.
3. Bestimme das multiplikative Inverse $[d]$ von $[e] \in \mathbb{Z}/\varphi(n)$.

Der RSA-Algorithmus

1. Nehme zwei Primzahlen große p, q und setze $n = p \cdot q$.
2. Wähle beliebiges $e \in \{2, \ldots, n-1\}$, mit $\mathrm{ggT}(e, n) = 1$.
3. Bestimme das multiplikative Inverse $[d]$ von $[e] \in \mathbb{Z}/\varphi(n)$.

öffentlicher Schlüssel: (e, n) privater Schlüssel: (d, n)

$$E : \mathbb{Z}/n \to \mathbb{Z}/n, g \mapsto g^e$$

Der RSA-Algorithmus

Verschlüsselung

Bob:

Abstrakt	Konkret
Wähle p, q. Setze $n = p \cdot q$	$p = 3, q = 11, n = 33$

Alice möchte Bob die Nachricht ’4’ schicken.

Der RSA-Algorithmus

Verschlüsselung

Bob:

Abstrakt

Wähle p, q. Setze $n = p \cdot q$
Wähle e: $(e, \varphi(n)) = 1$

Konkret

$p = 3, q = 11, n = 33$
Wähle $e = 7$. Checke $(7, 20) = 1$!

Alice möchte Bob die Nachricht ’4’ schicken.

Der RSA-Algorithmus

Verschlüsselung

Bob:

Abstrakt

Wähle p, q. Setze $n = p \cdot q$
Wähle e: $(e, \varphi(n)) = 1$
Finde das mult. Inverse $[d]$ von $[e]$ in $\mathbb{Z}/\varphi(n)$.

Konkret

$p = 3, q = 11, n = 33$
Wähle $e = 7$. Checke $(7, 20) = 1$!
Errechne $d = [3]$. Privat: $(3, 33)$
Veröffentliche: $(7, 33)$

Alice möchte Bob die Nachricht '4' schicken.

Der RSA-Algorithmus

Verschlüsselung

Bob:

Abstrakt

Wähle p, q. Setze $n = p \cdot q$
Wähle e: $(e, \varphi(n)) = 1$
Finde das mult. Inverse $[d]$ von $[e]$ in $\mathbb{Z}/\varphi(n)$.

Konkret

$p = 3, q = 11, n = 33$
Wähle $e = 7$. Checke $(7, 20) = 1$!
Errechne $d = [3]$. Privat: $(3, 33)$
Veröffentliche: $(7, 33)$

Alice möchte Bob die Nachricht '4' schicken.

Abstrakt

Suche Bobs öffentlichen Schlüssel

Konkret

Bobs öff. Schlüssel ist $(7, 33)$

Der RSA-Algorithmus

Verschlüsselung

Bob:

Abstrakt

Wähle p, q. Setze $n = p \cdot q$
Wähle e: $(e, \varphi(n)) = 1$
Finde das mult. Inverse $[d]$ von $[e]$ in $\mathbb{Z}/\varphi(n)$.

Konkret

$p = 3, q = 11, n = 33$
Wähle $e = 7$. Checke $(7, 20) = 1$!
Errechne $d = [3]$. Privat: $(3, 33)$
Veröffentliche: $(7, 33)$

Alice möchte Bob die Nachricht '4' schicken.

Abstrakt

Suche Bobs öffentlichen Schlüssel
Betrache $[m] \in \mathbb{Z}/n$ und berechne $[m]^e = [c]$.

Konkret

Bobs öff. Schlüssel ist $(7, 33)$
Betrachte $[4]$ als Element in $\mathbb{Z}/33$
Berechne $[4]^7 = [16]$

Der RSA-Algorithmus

Verschlüsselung

Bob:

Abstrakt

Wähle p, q. Setze $n = p \cdot q$
Wähle e: $(e, \varphi(n)) = 1$
Finde das mult. Inverse $[d]$ von $[e]$ in $\mathbb{Z}/\varphi(n)$.

Konkret

$p = 3, q = 11, n = 33$
Wähle $e = 7$. Checke $(7, 20) = 1$!
Errechne $d = [3]$. Privat: $(3, 33)$
Veröffentliche: $(7, 33)$

Alice möchte Bob die Nachricht '4' schicken.

Abstrakt

Suche Bobs öffentlichen Schlüssel
Betrache $[m] \in \mathbb{Z}/n$ und berechne $[m]^e = [c]$.

Konkret

Bobs öff. Schlüssel ist $(7, 33)$
Betrachte $[4]$ als Element in $\mathbb{Z}/33$
Berechne $[4]^7 = [16]$

Alice sendet '16' an Bob!

Der RSA-Algorithmus

Entschlüsselung

Bob erhält das Chiffrat ’16’:

Abstrakt

Berechne $[c]^d$ in $\mathbb{Z}/n$, denn

$$[c]^d = ([m]^e)^d = [m]^{k\varphi(n)+1} = [m].$$

Konkret

In $\mathbb{Z}/33$ gilt

$$[16]^3 = [25] \cdot [16] = [400] = [4].$$

Der RSA-Algorithmus

Entschlüsselung

Bob erhält das Chiffrat ’16’:

Abstrakt

Berechne $[c]^d$ in $\mathbb{Z}/n$, denn

$$[c]^d = ([m]^e)^d = [m]^{k\varphi(n)+1} = [m].$$

Konkret

In $\mathbb{Z}/33$ gilt

$$[16]^3 = [25] \cdot [16] = [400] = [4].$$

Bob erkennt den Klartext: ’4’.

Der RSA-Algorithmus

Wo steckt die Sicherheit?

1. RSA-Problem

m ausrechnen, wenn man n, e und m^e kennt.

1. Das RSA-Problem:

Kenne Chiffrat $c = m^e$ und öff. Schlüssel (e, n). Möchte m ermitteln!

Der RSA-Algorithmus

Wo steckt die Sicherheit?

1. RSA-Problem

m ausrechnen, wenn man n, e und m^e kennt.

$\leq$

2. Allg. RSA-Prob.

d ausrechnen, wenn man n und e kennt.

2. Das allgemeine RSA-Problem:

Kenne Chiffrat den öffentlichen Schlüssel (e, n). Möchte den geheimen Schlüssel d ermitteln!

Der RSA-Algorithmus

Wo steckt die Sicherheit?

1. RSA-Problem
m ausrechnen, wenn man n, e und m^e kennt.

$\leq$

2. Allg. RSA-Prob.
d ausrechnen, wenn man n und e kennt.

$=$

2'. $\varphi(n)$-Prob..
$\varphi(n)$ ausrechnen.

2'. Das φ-Problem:
Möchte effizient die Euler'sche φ-Funktion berechnen.

Der RSA-Algorithmus

Wo steckt die Sicherheit?

1. RSA-Problem
m ausrechnen, wenn man n, e und m^e kennt.

$\leq$

2'. $\varphi(n)$-Prob.
$\varphi(n)$ ausrechnen.

$\leq$

3. Faktorisieren
n in Primfaktoren zerlegen.

3. Das Faktorisierungsproblem:
Möchte für n effizient die Primfaktorzerlegung finden.

Der RSA-Algorithmus

Wo steckt die Sicherheit?

1. RSA-Problem

m ausrechnen, wenn man n, e und m^e kennt.

$\leq$

3. Faktorisieren

n in Primfaktoren zerlegen.

$\Rightarrow$ RSA zu brechen ist also höchstens so schwierig wie das Faktorisierungsproblem!

Der RSA-Algorithmus

Wo steckt die Sicherheit?

Und mindestens? Zahlen wie

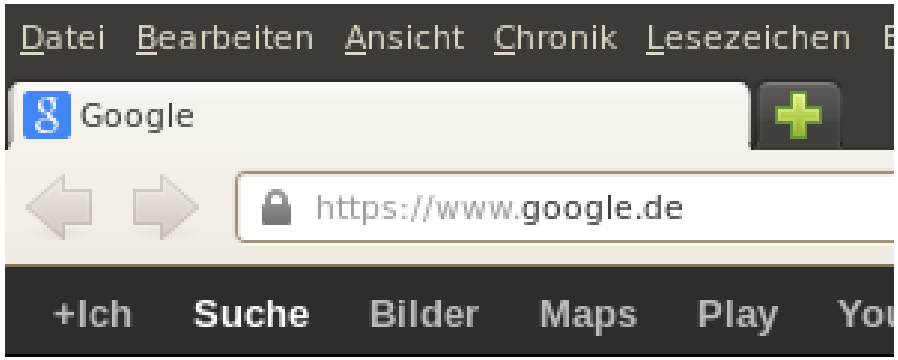
$$n = 75489763393055314128289985760068186621492280562287920094260074153209517236970341572518559797153449465576145454201026891283601494488262771597328435528850907122893849517975920947769168699513594157953875730587323943476340412264776041510220894422630321715512241190592912467594811186260668310257307289597639739 39$$

in seine zwei Primfaktoren zu zerlegen gilt trotz aller mathematischen Anstengungen noch immer als schwierig.

Der RSA-Algorithmus

Wo wird RSA tatsächlich verwendet?

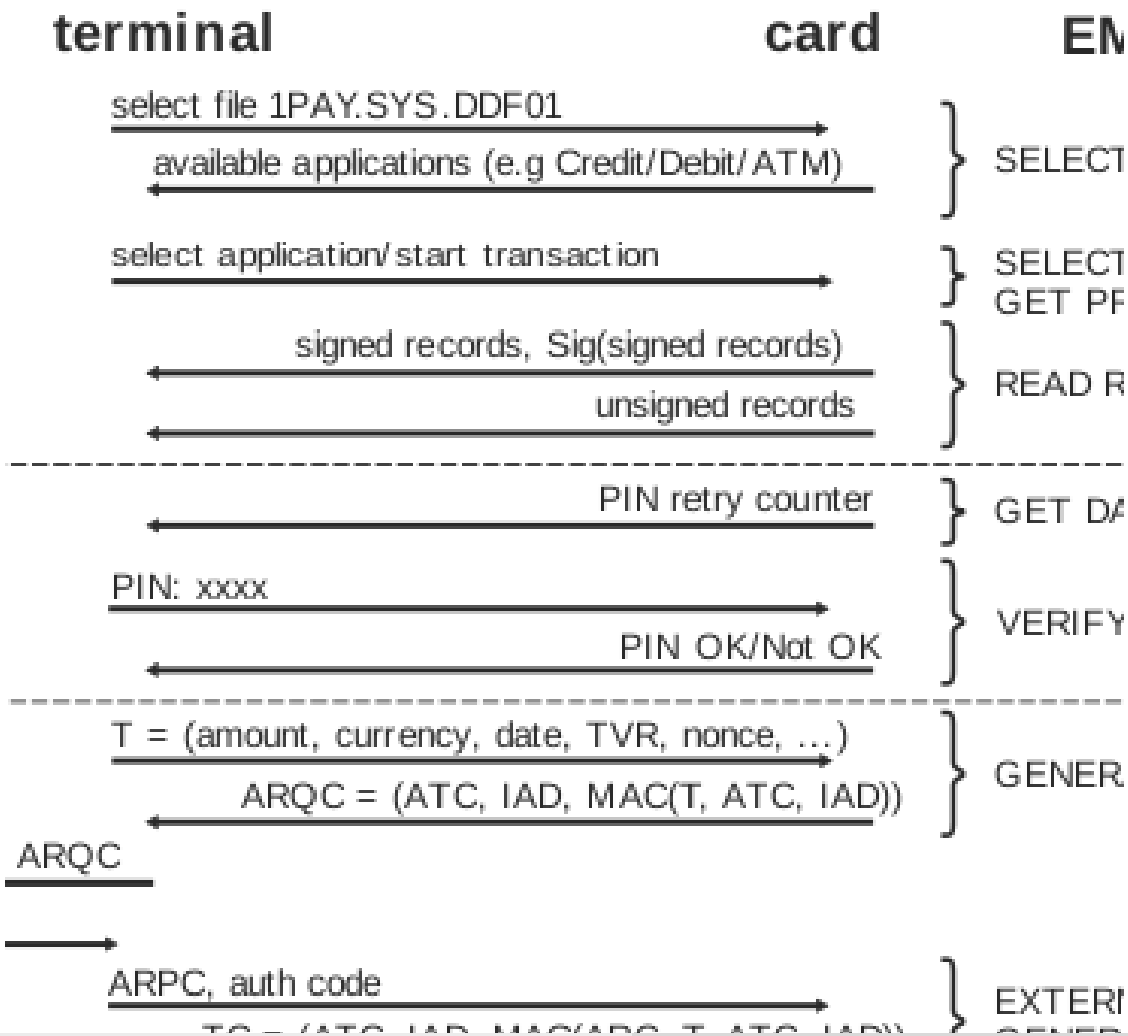
- SSL/TLS Verbindungen



Der RSA-Algorithmus

Wo wird RSA tatsächlich verwendet?

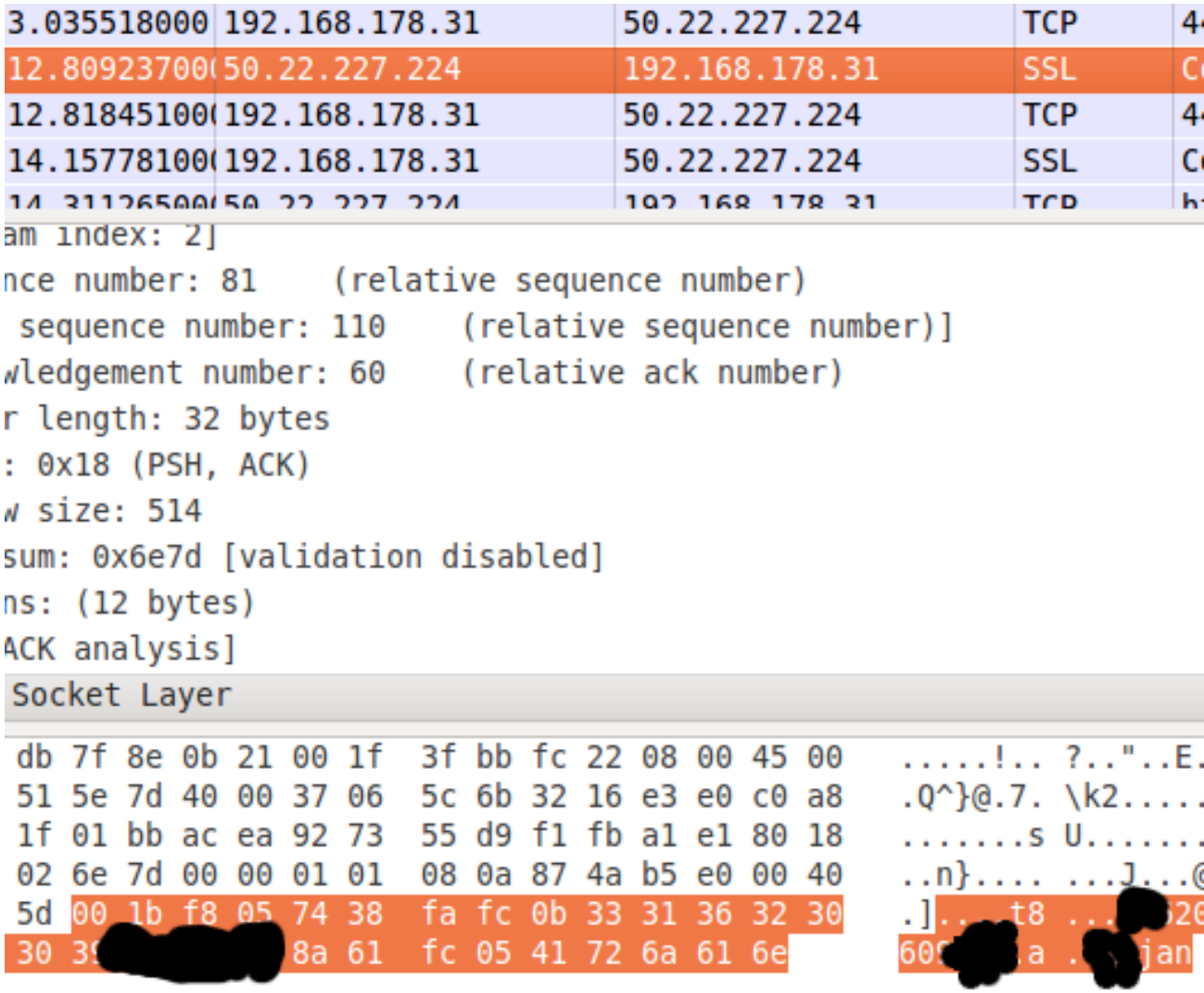
- SSL/TLS Verbindungen
- Kreditkarte/EMV



Der RSA-Algorithmus

Wo wird RSA tatsächlich verwendet?

- SSL/TLS Verbindungen
- Kreditkarte/EMV
- Whatsapp? Ups!



Zusammenfassung

- Was haben wir gesehen?

- Einblicke in symmetrische und public key Kryptographie.
- Eine einfache Kryptoanalyse.
- $\mathbb{Z}/n$ benutzen wir täglich, nicht nur in der Vorlesung!

Zusammenfassung

- Was haben wir gesehen?
- Welche Mathematik haben wir ausgeblendet?

- Primzahlen (Häufigkeiten, Suche,..)
- 'effizient', 'leicht', 'schwierig'
- Euklidischer Algorithmus, modulares Potenzieren, Satz von Euler-Fermat,...

Zusammenfassung

- Was haben wir gesehen?
- Welche Mathematik haben wir ausgeblendet?
- Attacken/Schulprojekte/Implementierungsfehler...

... und vieles mehr, auf meiner Homepage:
math.uni-hh▷personen▷PH▷Lehre▷Anwendungen der LA

Zusammenfassung

- Was haben wir gesehen?
- Welche Mathematik haben wir ausgeblendet?
- Attacken/Schulprojekte/Implementierungsfehler...

... und vieles mehr, auf meiner Homepage:
math.uni-hh▷personen▷PH▷Lehre▷Anwendungen der LA

Viele Dank für die Aufmerksamkeit!