Kryptographie

Martin Kreuzer

Fakultät für Informatik und Mathematik

Universität Passau

martin.kreuzer@uni-passau.de

Regionale Lehrerfortbildung

Passau, 21.12.2010

Inhaltsübersicht

1. Was ist Kryptographie?
2. Symmetrische Kryptosysteme
3. Polyalphabetische Verschlüsselungen
4. Public Key Kryptographie
5. Protokolle
6. Algebraische Angriffe

1 – Was ist Kryptographie?

Mullah Nasruddin sprach:

Ich kann Dir das Geheimnis des Universums nicht verraten,
denn dann wäre es ja kein Geheimnis mehr.

$\kappa\,\varrho\,\upsilon\,\pi\,\tau\,o\,\varsigma$	**cryptos**	das Verborgene
$\gamma\,\varrho\,\alpha\,\varphi\,\eta\,\iota\,\nu$	**graphein**	schreiben
$\lambda\,o\,\gamma\,o\,\varsigma$	**logos**	die Rede, die Lehre
$\alpha\,\nu\,\alpha\,\lambda\,\upsilon\,\sigma\,\iota\,\varsigma$	**analysis**	die Auflösung
$\sigma\,\tau\,\eta\,\gamma\,\alpha\,\nu\,o\,\varsigma$	**steganos**	bedeckt, versteckt

Kryptosysteme

Ein **Kryptosystem** besteht aus den folgenden Teilen:

(a) Einem **Alphabet** für den Klartext. Es heißt auch die Menge der **Klartexteinheiten** $\mathcal{M}$.

(b) Einer Menge von **Geheimtexteinheiten** $\mathcal{C}$.

(c) Einer Menge von **Geheimschlüsseln** $\mathcal{K}$.

(d) Für jedes $k \in \mathcal{K}$, einer **Verschlüsselungsabbildung**
$\epsilon_k : \mathcal{M} \longrightarrow \mathcal{C}$.

(e) Für jedes $k \in \mathcal{K}$, einer **Entschlüsselungsabbildung**
$\delta_k : \mathcal{C} \longrightarrow \mathcal{M}$ mit $\delta_k \circ \epsilon_k = \mathrm{id}$.

Definition 1.1 **(a)** *Wenn beide Parteien den Geheimschlüssel k kennen müssen um die Verschlüsselung ϵ_k bzw. die Entschlüsselung δ_k auszuführen, spricht man von einem* **symmetrischen Kryptosystem**.

(b) *Hängt die Verschlüsselungsabbildung nicht vom Geheimschlüssel ab, so liegt ein* **asymmetrisches** *oder* **Public Key Kryptosystem** *vor.*

2 – Symmetrische Kryptosysteme

Kein Kryptosystem is narrensicher gegenüber talentierten Narren.

Die einfachsten Kryptosysteme verwenden die **Substitution**: ersetze einen Buchstaben (oder eine Silbe, ein Wort, ...) durch einen festen anderen Buchstaben (oder ein Zeichen, ...).

Beispiel 2.1 (Caesar-Verschlüsselung)
Ersetze jeden Buchstaben durch den im Alphabet drei Stellen weiter liegenden (und verwende $X \mapsto A$, $Y \mapsto B$, $Z \mapsto C$).

QUINTILI VARE LEGIONES REDDE
$\longrightarrow$ **TXLQWLOL YDUH OHJLRQHV UHGGH**

Beispiel 2.2 **(Die Tafeln des Polybius)**

Zuerst ordnet man die Buchstaben in einer 5x5 Matrix an:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Nun ersetzt man jeden Buchstaben durch seine Zeilen- und Spaltennummer. Somit erhalten wir z.B.

POLYBIUS $\longrightarrow$ **35 34 31 54 12 24 45 43**

Wie man Substitutionen knackt

Klappt die Kryptoanalyse?
Nicht immer, aber immer öfter.

Wenn bei einem Verschlüsselungssystem jeder Klartextbuchstabe stets durch das gleiche Geheimtextzeichen ersetzt wird, spricht man von einer **monoalphabetischen** Verschlüsselung.

Ein solches System kann man mit der **Häufigkeitsanalyse** brechen. Diese Methode wurde ca. 850 in Bagdad veröffentlicht von

Abu Yusuf Yaqub ibn Is-haq ibn as Sabbah ibn 'Omran ibn Ismail Al-Kindi (805 – 873 n.Chr.)

Er schrieb ein Buch mit dem Titel

Risalah fi Istikhraj al-Mu'amma

Manuskript für die Entschlüsselung verschlüsselter Nachrichten

Al-Kindi war hauptberuflich Philosoph und Mathematiker am

Haus der Weisheit

der Kaliphen von Bagdad.

Also schrieb Al-Kindi ...

Eine Methode eine verschlüsselte Nachricht zu knacken, wenn wir ihre Sprache kennen, besteht darin einen **Klartext** in derselben Sprache zu finden, der mindestens eine Seite lang ist. Darin zählen wir die Häufigkeit jedes einzelnen Buchstaben.

Den am häufigsten vorkommenden Buchstaben nennen wir den "ersten", den nächsthäufigsten den "zweiten", den folgenden den "dritten", und so weiter, bis wir alle im Klartextbeispiel vorkommenden Buchstaben abgearbeitet haben.

Jetzt betrachten wir den verschlüsselten Text und klassifizieren seine Symbole ebenso. Das am häufigsten auftretende Symbol wandeln wir in den "ersten" Buchstaben um, das nächsthäufigste Symbol in den "zweiten" Buchstaben, und so weiter, bis wir alle Symbole in der verschlüsselten Nachricht abgearbeitet haben.

Legrand versus Captain Kidd

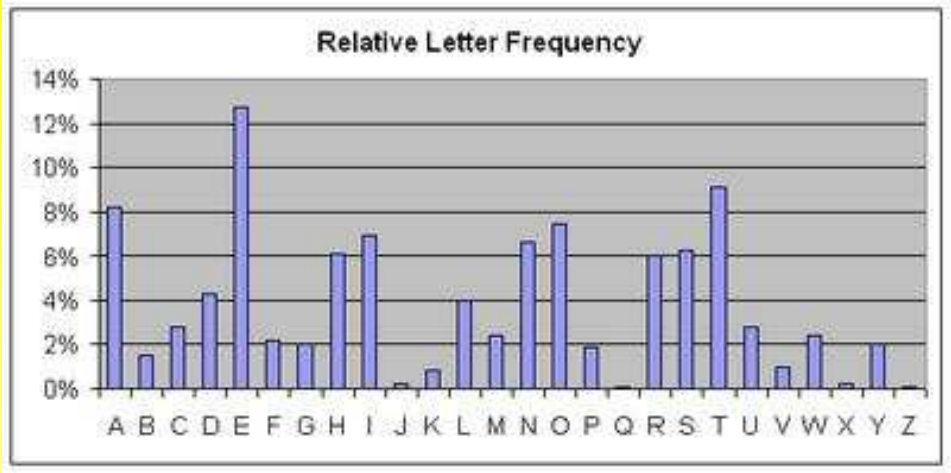
Beispiel einer Häufigkeitsanalyse *a la* Al-Kindi

In Edgar Allan Poes Erzählung "Der Goldkäfer" erhält der Held Legrand folgende verschlüsselte Nachricht:

53 ≠≠ †	305))	6∗; 48	26)4 ≠	.)4 ≠)	; 806∗	; 48 † 8
]/60)	)85; 1	≠ (; :≠	∗8 † 83	(88)5	∗†; 46	(; 88∗
96∗?;	8)∗ ≠ (	; 485)	; 5 ∗ †2	: ∗ ≠ (;	4956∗	2(5 ∗ −
4)8]/	8∗; 40	69285	);)6†	8)4 ≠≠	; 1(≠ 9	; 4808
1; 8 : 8	/1; 48	†85; 4	)485†	52880	6 ∗ 81(	/9; 48
; (88;	4(≠?3	4; 48)	4 ≠; 16	1; : 18	8; ≠?;	

Wegen einer Markierung weiß er, dass sie von dem berühmten Seeräuber Captain Kidd stammt und in Englisch verfasst wurde.

Die Häufigkeitstabelle der englischen Sprache ist:



Wir folgen al-Kindi und erstellen eine Häufigkeitstafel der Symbole:

1. 8	2. ;	3. 4	4.)	5. $\neq$	6. $*$	7. 5	8. 6	9. (
16.5%	13%	9.5%	8.5%	7%	6.5%	6%	5.5%	5%

Auf jeden Fall sollte also $8 \mapsto E$ und $; \mapsto T$ gelten.

Damit erhalten wir folgende Teilentschlüsselung:

$53 \neq\neq \dagger$	$305))$	$6 * T4E$	$26)4 \neq$	$.)4 \neq)$	$TE06*$	$T4E \dagger E$
$]/60)$	$)E5T1$	$\neq (T :\neq$	$*E \dagger E3$	$(EE)5$	$* \dagger T46$	$(TEE*$
$96*?T$	$E)* \neq ($	$T4E5)$	$T5 * \dagger 2$	$: * \neq (T$	$4956*$	$2(5 * -$
$4)E]/$	$E * T40$	$692E5$	$)T)6\dagger$	$E)4 \neq\neq$	$T1(\neq 9$	$T4E0E$
$1TE : E$	$/1T4E$	$\dagger E5T4$	$)4E5\dagger$	$52EE0$	$6 * E1($	$/9T4E$
$T(EET$	$4(\neq?3$	$4T4E)$	$4 \neq T16$	$1T : 1E$	$ET \neq?T$	

Wegen des siebenmaligen Auftretens der Kombination $T4E$ liegt es nahe, $4 \mapsto H$ zu vermuten, was mit der Häufigkeitstabelle verträglich ist. Wir erhalten eine neue Teilentschlüsselung:

$53 \neq\neq \dagger$	$305))$	$6*THE$	$26)H \neq$	$.)H \neq)$	$TE06*$	$THE\dagger E$
$]/60)$	$)E5T1$	$\neq (T :\neq$	$*E \dagger E3$	$(EE)5$	$* \dagger TH6$	$(TEE*$
$96*?T$	$E)* \neq ($	$THE5)$	$T5 * \dagger 2$	$: * \neq (T$	$H956*$	$2(5 * -$
$H)E]/$	$E*TH0$	$692E5$	$)T)6\dagger$	$E)H \neq\neq$	$T1(\neq 9$	$THE0E$
$1TE{:}E$	$/1THE$	$\dagger E5TH$	$)HE5\dagger$	$52EE0$	$6 * E1($	$/9THE$
$T(EET$	$H(\neq?3$	$HTHE)$	$H\neq T16$	$1T : 1E$	$ET \neq?T$	

Jetzt zeigt der Anfang der letzten Zeile ($\mapsto R$ (bei 5% vs. 6.5%) und dann liefert das Ende der zweiten Zeile das Wort “thirteen”, also $6 \mapsto I$ (bei 5.5% vs. 6.5%) sowie $* \mapsto N$ (bei 6% vs. 7%).

Unser Zwischenresultat lautet jetzt:

$53 \neq\neq \dagger$	$305))$	$INTHE$	$2I)H \neq$	$.)H \neq)$	$TE0IN$	$THE\dagger E$
$]/I0)$	$)E5T1$	$\neq RT:\neq$	$NE\dagger E3$	$REE)5$	$N\dagger THI$	$RTEEN$
$9IN?T$	$E)N \neq R$	$THE5)$	$T5N \dagger 2$	$:N \neq RT$	$H95IN$	$2R5N-$
$H)E]/$	$ENTH0$	$I92E5$	$)T)I\dagger$	$E)H \neq\neq$	$T1R \neq 9$	$THE0E$
$1TE:E$	$/1THE$	$\dagger E5TH$	$)HE5\dagger$	$52EE0$	$INE1R$	$/9THE$
$TREET$	$HR \neq ?3$	$HTHE)$	$H \neq T1I$	$1T:1E$	$ET \neq ?T$	

Die letzte Zeile “tree thr...h the” macht nur für “through” Sinn, also $\neq \mapsto O$ (bei 7% vs. 8%) und $? \mapsto U$ (bei 1.5% vs. 3%) sowie $3 \mapsto G$ (bei 2% vs. 1.5%). Dann muss die Fortsetzung “through the .hot” mit “shot” ergänzt werden, da nur “a” und “s” häufig genug sind. Dies liefert $) \mapsto S$ (bei 8.5% vs. 6%). Schließlich bleibt für das “a” nur $5 \mapsto A$ übrig (bei 6% vs. 8%). Jetzt lautet der Zwischenstand:

AGOO†	G0ASS	INTHE	2ISHO	.SHOS	TE0IN	THE†E
]/I0S	SEAT1	ORT:O	NE†EG	REESA	N†THI	RTEEN
9INUT	ESNOR	THEAS	TAN†2	:NORT	H9AIN	2RAN–
HSE]/	ENTH0	I92EA	STSI†	ESHOO	T1RO9	THE0E
1TE:E	/1THE	†EATH	SHEA†	A2EE0	INE1R	/9THE
TREET	HROUG	HTHES	HOT1I	1T:1E	ETOUT	

Von hier aus ist es ein Leichtes, den Text zu vervollständigen:

A good glass in the bishop's hostel in the devil's seat
forty one degrees and thirteen minutes northeast and by north
main branch seventh limb east side
shoot from the left eye of the death's head a bee line
from the tree trough the shot fifty feet out.

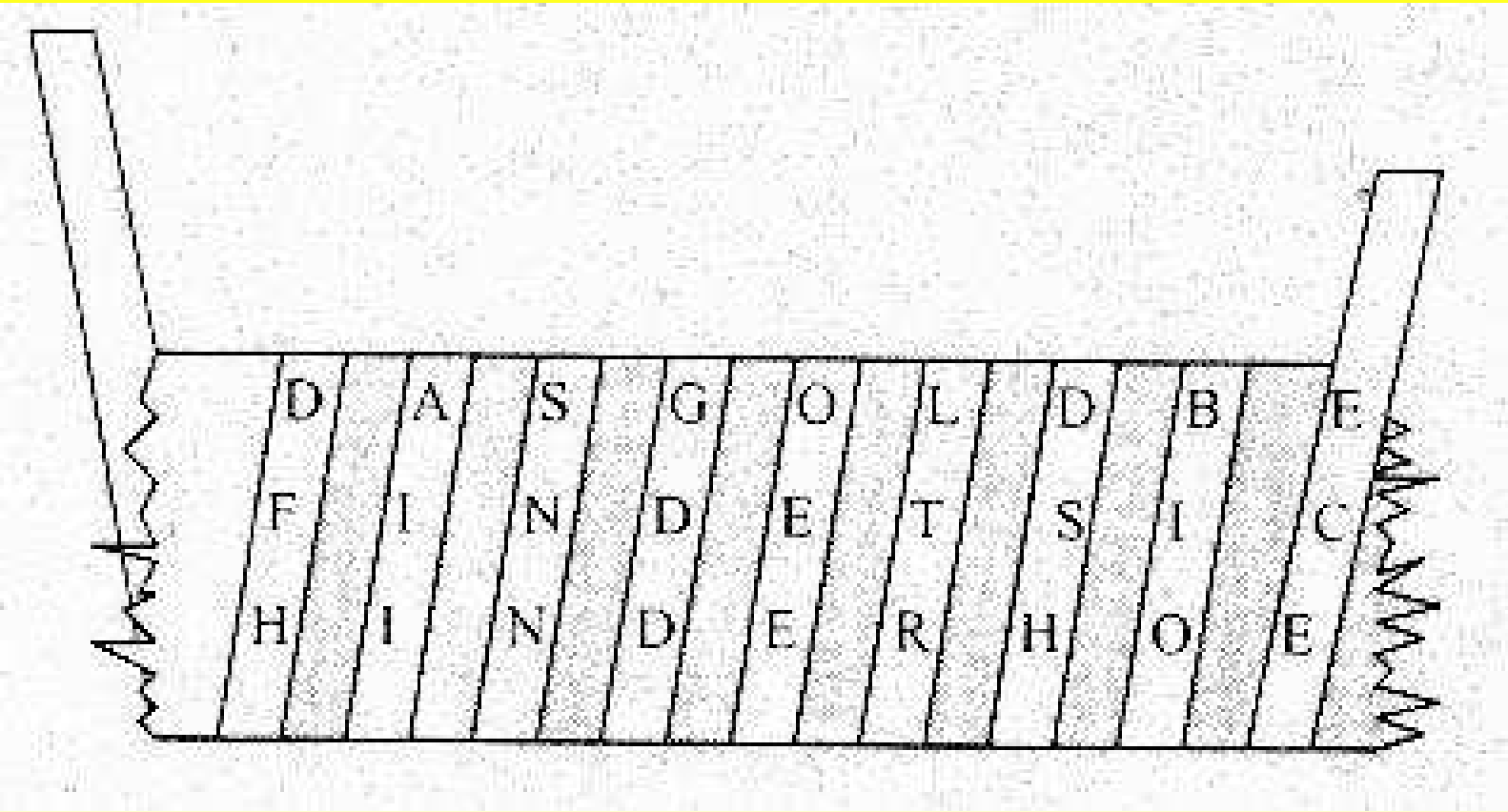
Transpositionen

Das sind meine Prinzipien.
Und wenn sie Ihnen nicht passen,
dann habe ich noch andere.
(Groucho Marx)

Ein anderes Prinzip der Verschlüsselung ist die Buchstaben zu vertauschen. Man nennt solche Systeme **Transpositionen**.

Beispiel 2.3 **(Die Skytale)**
Die Skytale war der erste kryptographische Apparat und wurde ca. 475 v.Chr. in Sparta entwickelt.

Ein Papierstreifen wird um einen Stab gewickelt und mit der geheimen Nachricht beschrieben. Nach dem Abwickeln sind die Buchstaben vertauscht. Der geheime Schlüssel ist die Stabdicke.



Verschlüsselte Nachricht: HFDIIANNSDDGEEORTLHSDOIBECE

Beispiel 2.4 (Spaltentranspositionen)

Bei der **Spaltentransposition mit Kennwort** *wird zuerst der Klartext zeilenweise in eine Matrix fest vereinbarter Größe geschrieben.*

E	S	W	A
R	S	C	H
O	N	D	U
N	K	E	L

Dann wird die Matrix spaltenweise ausgelesen, wobei das Kennwort angibt, in welcher Reihenfolge die Spalten ausgelesen werden. Die Position der Buchstaben des Kennworts im Alphabet bestimmt diese Reihenfolge.

Das Kennwort **DAME** entspricht somit der Reihenfolge **(2,1,4,3)**.
Aus

E	S	W	A
R	S	C	H
O	N	D	U
N	K	E	L

wird dann der Geheimtext

SSNK ERON AHUL WCDE

Wie man Transpositionen knackt

Optimist: Wenn sich die Wirtschaft so weiterentwickelt, werden wir alle bald auf der Straße betteln.

Pessimist: Von wem?

Um Transpositionen zu knacken verwendet man die Häufigkeiten von **Bigrammen**, d.h. von 2-Buchstaben-Kombinationen.

Beispielhaft knacken wir den Geheimtext **SSNK ERON AHUL WCDE** der obigen Spaltentransposition mit Kennwort. Zuerst schreiben wir ihn in die Spalten einer geeigneten Matrix. Hier bietet sich eine 4x4 Matrix an.

S	E	A	W
S	R	H	C
N	O	U	D
K	N	L	E

Nun wählen wir eine Spalte mit vielen häufigen Buchstaben, z.B. **ERON** und stellen sie mit den anderen Spalten zusammen:

ES	1,4%		EA	0,26%		EW	0,23%
RS	0,54%		RH	0,19%		RC	0,09%
ON	0,65%		OU	0,1%		OD	0,07%
NK	0,25%		NL	0,05%		NE	1,22%

Offensichtlich ist die erst Kombination die wahrscheinlichste. Nun stellen wir die zweite Spalte den verbleibenden gegenüber und erhalten

SA	0,96%		SW	0,1%
SH	0,09%		SC	0,89%
NU	0,33%		ND	1,87%
KL	0,1%		KE	0,26%

Hier ist die zweite Kombination wahrscheinlicher.

So fahren wir fort. Geraten wir in eine "Sackgasse", können wir auf der anderen Seite fortfahren, also neue Spalten vorne anstellen.

Schließlich können wir den Klartext zeilenweise aus der Matrix auslesen.

3 – Polyalphabetische Verschlüsselungen

Das Geheimnis der Kreativität ist das Wissen darum,
wie man seine Quellen verbirgt.
(Albert Einstein)

Die erste **polyalphabetische Verschlüsselung** wurde 1466 beschrieben von **Leon Battista Alberti** in seinem Buch

De Componendis Cifris
(Anleitung zum Verschlüsseln von Texten)

und später u.a. von **Blaise de Vigenere** und anderen weiterentwickelt. Eine einfache Version dieses Verfahrens funktioniert wir folgt:

(1) Wähle ein **Schlüsselwort**, z.B. **KATZE**. Es entspricht Verschiebungen des Alphabets um $(10, 0, 19, 25, 4)$ Buchstaben.

(2) Schreibe den Klartext und die Verschiebungen untereinander:

S	E	N	D	E	T	B	I	T	T	E	H	I	L	F	E
10	0	19	25	4	10	0	19	25	4	10	0	19	25	4	10

(3) Wende die Verschiebungen an und erhalte den Geheimtext

$$C \quad E \quad G \quad C \quad I \quad D \quad B \quad B \quad S \quad X \quad O \quad H \quad B \quad K \quad J \quad O$$

Ein fester Buchstabe, z.B. **E** wird immer wieder anders verschlüsselt, d.h. das System ist **polyalphabetisch**. Wie knackt man eine solche Verschlüsselung?

Der Kasiski-Test

dient dazu, die Schlüsselwortlänge zu finden. **Friedrich Wilhelm Kasiski** (1805 – 1881) war ein pensionierter Offizier des 33. Preußischen Infantrieregiments.

1863 schrieb er das Buch

Die Geheimschriften und die Dechiffrier-Kunst

Darin erklärte er, wie man Vigenere Kryptosysteme mit wiederholendem Schlüsselwort knacken kann, aber keiner interessierte sich dafür.

Kasiski wandte sich daraufhin der Amateur-Anthropologie und der Amateur-Archäologie zu. Er starb ohne jemals zu erfahren, dass er die Kryptoanalyse revolutioniert hatte.

Idee: Kommt zweimal derselbe Buchstabe oder dieselbe Buchstabenfolge im Klartext vor (z.B. das Wort **der**) und ist der Abstand durch die Schlüsselwortlänge teilbar, so wird jeweils gleich verschlüsselt.

(1) Suche also im Geheimtext Folgen von drei oder mehr Buchstaben, die mehrfach vorkommen.

(2) Bestimme die Abstände dieser Buchstabengruppen.

(3) Der **ggT** möglichst vieler dieser Abstände ist höchstwahrscheinlich die Schlüsselwortlänge ℓ.

(4) Die Buchstaben 1, $\ell + 1$, $2\ell + 1$, etc. werden nun alle mit der gleichen Verschiebung verschlüsselt. Führe eine Häufigkeitsanalyse durch und finde diese Verschiebung!

Der Friedman-Test

beruht ebenfalls auf sehr einfachen kombinatorischen Überlegungen, die man mit den Mitteln der Schulmathematik nachvollziehen kann. Er liefert eine Formel für die wahrscheinlichste Schlüsselwortlänge beim Vigenere-System.

Definition 3.1 *Aus einem Text wählt man zufällig zwei Buchstaben aus. Die Wahrscheinlichkeit dafür, dass man zweimal den gleichen Buchstaben erwischt, heißt der* **Friedmansche Koinzidenzindex** p_F *des Texts.*

Bei deutschen Texten gilt $p_F \approx 7,62\%$.

Bei zufälligen Texten gilt $p_F \approx 3,85\%$.

Bei einer monoalphabetischen Verschlüsselung bleibt p_F erhalten, bei polyalphabetischer Verschlüsselung nimmt p_F i.A. ab.

Satz 3.2 *Ein Vigenere-verschlüsselter Text der Länge m habe den Koinzidenzindex p_F. Der Klartext habe den Koinzidenzindex p_L. Dann gilt für die Schlüsselwortlänge ℓ die Beziehung*

$$\ell \approx (p_L - 1/26)\, m \,/\, ((m-1)p_F - m/26 + p_L)$$

Beweis: Setze den Geheimtext $(c_1, \ldots, c_m)$ in eine Matrix mit ℓ Spalten:

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_\ell \\ c_{\ell+1} & c_{\ell+2} & \cdots & c_{2\ell} \\ \vdots & \vdots & & \vdots \end{pmatrix}$$

In jeder Spalte liegt eine monoalphabetische Verschlüsselung vor. Der Koinzidenzindex jeder Spalte ist also $\approx p_L$.

Für Paare aus verschiedenen Spalten ist die Wahrscheinlichkeit dafür, dass zwei gleiche Buchstaben vorliegen, etwa 1/26. Es gibt ca. $\binom{\ell}{2} \cdot (m/\ell)^2$ solche Paare.

Die Zahl der Paare, bei denen beide Buchstaben in der gleichen Spalte stehen, ist ca. $\ell \cdot \binom{m/\ell}{2}$.

Die Anzahl der Paare gleicher Buchstaben ist also etwa

$$A = \ell \cdot \binom{m/\ell}{2} \cdot p_F + \binom{\ell}{2} \cdot (m/\ell)^2 \cdot (1/26)$$

Wegen $p_F = A/\binom{m}{2}$ kann man nun nach ℓ auflösen und erhält die behauptete Formel. **q.e.d.**

4 – Die RSA-Verschlüsselung

Manche Menschen würden eher sterben
als selbständig zu denken,
und das tun sie dann auch.
(Bertrand Russell)

Rivest – Shamir – Adleman

1976: Ronald Rivest, Adi Shamir (zwei Informatiker) und Leonard Adleman (ein Mathematiker) suchen nach einer Funktion für die **Public Key Kryptographie**.

Die beiden Informatiker machen ein Jahr lang zahlreiche Vorschläge, der Mathematiker widerlegt sie.

April 1977: Rivest findet eine geeignete **Einweg-Funktion** und schreibt eine Forschungsarbeit.

Adleman will anfangs nicht als Koautor beteiligt sein. Dann gibt er nach unter der Bedingung, dass er als letzter genannt wird.

"Ich dachte, dies wäre die uninteressanteste Arbeit bei der ich jemals Koautor wäre."

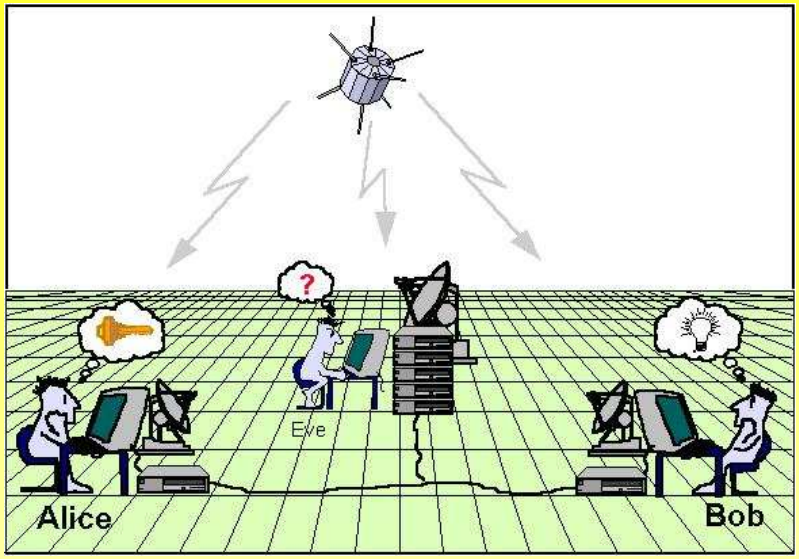
Feb. 1978: Der Artikel "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" erscheint in *Communications of the ACM*, Band 21, Seiten 120-126.

Das MIT erhält 5000 Anfragen nach Sonderdrucken der Arbeit.

Sep. 1983: US-Patent # 4,405,829 "Cryptographic Communications System and Method" für das RSA Kryptosystem

ab 1983: Die USA verhängen strenge Exportbeschränkungen für RSA. Der Einsatz ist strikt reglementiert und bleibt im wesentlichen auf Banken beschränkt.

Wie funktioniert RSA ?



Bob verschlüsselt seine Nachricht mit dem **Public Key** von Alice.
Eve hört mit, kann die Verschlüsselung aber nicht knacken.

Nur **Alice** kennt ihren **geheimen Schlüssel** und kann die Nachricht entschlüsseln.

Wie funktioniert RSA nun wirklich?

Geheim: Zwei Primzahlen p und q und eine Zahl e mit $10 < e < n = p \cdot q$.

Öffentlich: Das Produkt n und eine Zahl d mit $de \equiv 1 \pmod{(p-1)(q-1)}$.

Verschlüsselung: Verwandle die Nachricht in Zahlen m mit $m < n$. Berechne die Zahl $c = m^e \pmod{n}$ und sende sie.

Entschlüsselung: Berechne die Zahl $c^d \pmod{n}$ und erhalte m.

Korrektheit: Nach dem **Satz von Euler** gilt $c^d = (m^e)^d = m^{de} \equiv m^1 \pmod{n}$.

Sicherheit: Um p, q oder d zu berechnen muss man n in seine Primfaktoren zerlegen. Dies gilt als sehr schwierig.

Der kleine Satz von Fermat

Satz 4.1 *Sei p eine Primzahl und a eine nicht durch p teilbare Zahl. Dann gilt*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beweis: Wenn wir von a ein Vielfaches von p subtrahieren, bleibt $a^{p-1} \pmod{p}$ gleich. Also können wir $0 < a < p$ annehmen..

Betrachte nun die Reste $a \pmod{p}$, $2a \pmod{p}$, u.s.w. bis $(p-1)a \pmod{p}$. Dies sind $p-1$ verschiedene Zahlen im Bereich $\{1, \ldots, p-1\}$, denn wären zwei gleich, z.B.

$$i\,a \equiv j\,a \pmod{p}$$

so würde p das Produkt $(i-j)\,a$ teilen. Folglich würde p dann a oder $(i-j)$ teilen, was nicht geht, da beide Zahlen > 0 und $< p$ sind.

Somit sind diese Reste eine Permutation der Zahlen $\{1, \ldots, p-1\}$. Also ist ihr Produkt $1 \cdot 2 \cdots (p-1) = (p-1)!$, d.h. es gilt

$$a \cdot (2a) \cdots (p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$$

Folglich besitzt a^{p-1} den Rest 1 modulo p. **q.e.d.**

Satz 4.2 (Der Chinesische Restsatz)
Sind p, q teilerfremde Zahlen, so gibt es zu $a, b \in \mathbb{Z}$ genau ein $c \in \{0, \ldots, pq-1\}$ mit

$$c \equiv a \pmod{p} \quad \text{und} \quad c \equiv b \pmod{q}$$

Aus den Sätzen 4.1 und 4.2 folgt sofort der

Satz 4.3 (Satz von Euler) *Ist $n = pq$ Produkt zweier Primzahlen und $\mathrm{ggT}(a, n) = 1$, so gilt*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

Kann man RSA knacken?

Es macht irgendwie Spaß das Unmögliche zu tun.

(Walt Disney)

Selbst mit modernsten Computern und den besten bekannten Algorithmen kann man Zahlen n nicht in ihre Faktoren p und q zerlegen, wenn p und q mehr als 100 Stellen haben.

Es wurde aber trotz intensiver Bemühungen noch nicht **bewiesen**, dass die Aufgabe nicht in vernünftiger Zeit lösbar ist.

Stattdessen haben die Mathematiker bewiesen, dass man große Zahlen mit einem Quantencomputer **effizient** faktorisieren kann. Der Beweis ist aber schwierig.

5 – Protokolle

Frage nicht was Dein Land für Dich tun kann.
Frage was Dein Land für die großen Banken tut.

Ein **(kryptographisches) Protokoll** ist eine Folge von Anweisungen mit denen zwei (oder mehr) Parteien eine gewisse Aufgabe erledigen wollen, z.B. Schlüsselvereinbarung, Authentifikation, elektronische Signatur, u.s.w.

Das erste wichtige Protokoll war die **Diffie-Hellman Schlüsselvereinbarung**. Dabei wollen zwei Parteien **A** und **B** über einen öffentlichen Kanal einen gemeinsamen Geheimschlüssel vereinbaren.

Diffie-Hellman Schlüsselvereinbarung

(1) **A** und **B** einigen sich auf eine große Primzahl p und eine Zahl g deren Potenzen alle Reste modulo p (außer $\bar{0}$) durchlaufen.

(2) **A** wählt eine Zufallszahl a und **B** wählt eine Zufallszahl b.

(3) **A** berechnet $x = g^a \pmod{p}$ und **B** berechnet $y = g^b \pmod{p}$.

(4) **A** und **B** tauschen x und y aus.

(5) **A** berechnet $k = y^a \pmod{p}$ und **B** berechnet $k = x^b \pmod{p}$. (In beiden Fällen gilt $k = g^{ab} \pmod{p}$.)

Kann ein Angreifer **diskrete Logarithmen** berechnen, d.h. kann er aus $g^a \pmod{p}$ auf a schließen, so kann er den Geheimschlüssel k finden.

Angriffe auf Protokolle

Man-in-the-Middle Angriff: Der Angreifer **E** fängt die Nachrichten von **A** ab und leitet eigene Nachrichten an **B** weiter. Dann fängt er die Antworten von **B** ab und sendet eigene Antworten an **A** weiter.

Replay Angriff: Der Angreifer liest alle Nachrichten mit und sendet später noch einmal dieselbe Kommunikation an B. (Beispielsweise bei der Authentifikation gegenüber einem Computer mit dem Passwort-Verfahren.)

Denial-of-Service (DOS) Angriff: Der Angreifer sendet so viele Kommunikationsanfragen an **B**, dass der Rechner von **B** überlastet ist und zusammenbricht oder Fehler produziert.

6 – Algebraische Angriffe

Man kann nicht jemandem etwas beibringen
wenn sein Gehalt davon abhängt,
dass er es nicht kapiert.
(Upton Sinclair)

Man kann jede Verschlüsselungsfunktion betrachten als eine Abbildung, die einem 0-1-Tupel (dem **Klartext**) ein anderes (den **Geheimtext**) zuordnet.

Ist $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ der Körper mit zwei Elementen, so ist dies also eine Abbildung $\epsilon : (\mathbb{F}_2)^s \longrightarrow (\mathbb{F}_2)^n$.

Jede solche Abbildung ist durch **Polynome** gegeben, d.h. es gibt $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_n]$ mit $\epsilon(v) = (f_1(v), \ldots, f_s(v))$ für alle v.

Wir knacken zwei Runden DES

DES = **D**ata **E**ncryption **S**tandard (1977 – 2001)

AES = **A**dvanced **E**ncryption **S**tandard (seit 2001)

Betrachte die Verschlüsselungsfunktion von DES als Abbildung $\epsilon : (\mathbb{F}_2)^{64} \longrightarrow (\mathbb{F}_2)^{64}$.

Satz 6.1 *Zu jeder Abbildung* $\epsilon : (\mathbb{F}_2)^{64} \longrightarrow (\mathbb{F}_2)^{64}$ *gibt es* **Polynome** $f_1, \ldots, f_{64}$ *in 64 Unbestimmten mit*

$$\epsilon(x_1, \ldots, x_{64}) = (f_1(x_1, \ldots, x_{64}), \ldots, f_{64}(x_1, \ldots, x_{64}))$$

Wir führen eine **Known-Plaintext-Attacke** durch. Dazu nehmen wir an, dass wir ein Paar (Klartext, Geheimtext) kennen, z.B. weil das erste Byte einer pdf-Datei verschlüsselt wurde.

Dann schreiben wir die Verschlüsselungsfunktion in Abhängigkeit der 56 bits des Geheimschlüssels (Unbestimmte $k_0, \ldots, k_{55}$) und erhalten ein **algebraisches Gleichungssystem**

$$\begin{aligned} g_1(k_0, \ldots, k_{55}) &= 0 \\ &\vdots \\ g_{1120}(k_0, \ldots, k_{55}) &= 0 \end{aligned}$$

Zum Beispiel seien folgende Daten gegeben:

Klartext: [0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0];

Geheimtext: [1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0];

Gleichungssystem (1120 Gleichungen, 288 Unbestimmte):

$$
\begin{aligned}
& x[0,1]x[0,3]x[0,4] + x[0,2]x[0,3]x[0,4] + x[0,1]x[0,4]x[0,5] \\
+ \quad & x[0,3]x[0,4]x[0,5] + x[0,1]x[0,2]y[0,0] + x[0,1]x[0,3]y[0,0] \\
+ \quad & x[0,2]x[0,3]y[0,0] + x[0,1]x[0,4]y[0,0] + x[0,3]x[0,4]y[0,0] \\
+ \quad & x[0,2]x[0,5]y[0,0] + x[0,3]x[0,5]y[0,0] + x[0,1]x[0,2]y[0,1] \\
+ \quad & x[0,1]x[0,3]y[0,1] + x[0,2]x[0,3]y[0,1] + x[0,1]x[0,4]y[0,1] \\
+ \quad & x[0,3]x[0,4]y[0,1] + x[0,1]x[0,5]y[0,1] + x[0,4]x[0,5]y[0,1] \\
+ \quad & x[0,1]y[0,0]y[0,1] + x[0,4]y[0,0]y[0,1] + x[0,1]x[0,3]y[0,3] \\
+ \quad & x[0,2]x[0,3]y[0,3] + x[0,1]x[0,4]y[0,3] + x[0,2]x[0,4]y[0,3] \\
+ \quad & x[0,2]x[0,5]y[0,3] + x[0,3]x[0,5]y[0,3] + x[0,2]y[0,0]y[0,3]
\end{aligned}
$$

$$
\begin{aligned}
&+ \quad x[0,3]y[0,0]y[0,3] + x[0,4]y[0,0]y[0,3] + x[0,5]y[0,0]y[0,3] \\
&+ \quad x[0,1]y[0,1]y[0,3] + x[0,4]y[0,1]y[0,3] + y[0,0]y[0,1]y[0,3] \\
&+ \quad x[0,3]y[0,2] \;=\; 0,
\end{aligned}
$$

und weitere **1119** Gleichungen ....

Es ergibt sich $(k_0, \ldots, k_{55}) \;=\; (0,0,1,1,1,0,\ldots)$.

DES ist nicht mehr sicher!

Und an AES arbeiten wir!

Vielen Dank für Ihre Aufmerksamkeit!