# Glh Frghnqdfnhu jhvwhuq, khxwh, xhehuprujhq

**Martin Kreuzer**

**Fachbereich Mathematik**

**Universität Dortmund**

martin.kreuzer@uni-dortmund.de

**Zwischen Brötchen und Borussia**

**13. Mai 2006**

# Ein Ersatzmann für einen Professor?

Seine Magnifizenz Prof. Dr. Eberhard Becker

# Inhaltsübersicht

# 1 – Definitionen

Ein Crashkurs in Altgriechisch

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

# 2 – Die alten Knacker

(Kryptographie und Kryptoanalysis in der Antike)

## 2.1 Patentschutz durch Kryptographie

- ca. 1500 v.Chr. Seleucia am Tigris
- die erste Formel zur Herstellung einer Glasur für Tonwaren musste geschützt werden
- Verfahren: verwende Keilschriftzeichen in ihrer seltensten Bedeutung, streiche Konsonanten am Silbenende, buchstabiere das gleiche Wort auf verschiedene Weisen

## Ein Beispiel für den Keilschriftcode

(von George Bernard Shaw)

Im Englischen spricht man manchmal

| | | | | |
|---|---|---|---|---|
| *GH* | als | *F* | wie z.B. in | *tough* |
| *O* | als | *I* | wie z.B. in | *women* |
| *TI* | als | *SH* | wie z.B. in | *nation* |

Also kann man FISH auch schreiben als GHOTI!

## 2.2 Der erste namentlich bekannte Codeknacker

der Geschichte war der **Prophet Daniel**. Während des Exils der Judäer in Babylon gab **König Belsazar** ca. 540 v.Chr. ein Fest. Eine Geisterhand schrieb folgendes Kryptogramm an die Wand:

MENE MENE TEKEL UPHARSIN

Die versammelten Wissenschaftler des Königs konnten dieses nicht entschlüsseln, obwohl es in gewöhnlichem Aramäisch geschrieben war.


מנה מנה
תקל
פרסין

Das Menetekel des Belsazar hatte folgenden Wortlaut:

| MENE | MENE | TEKEL | UPHARSIN |
|---|---|---|---|
| gezählt | gezählt | gewogen | geteilt |

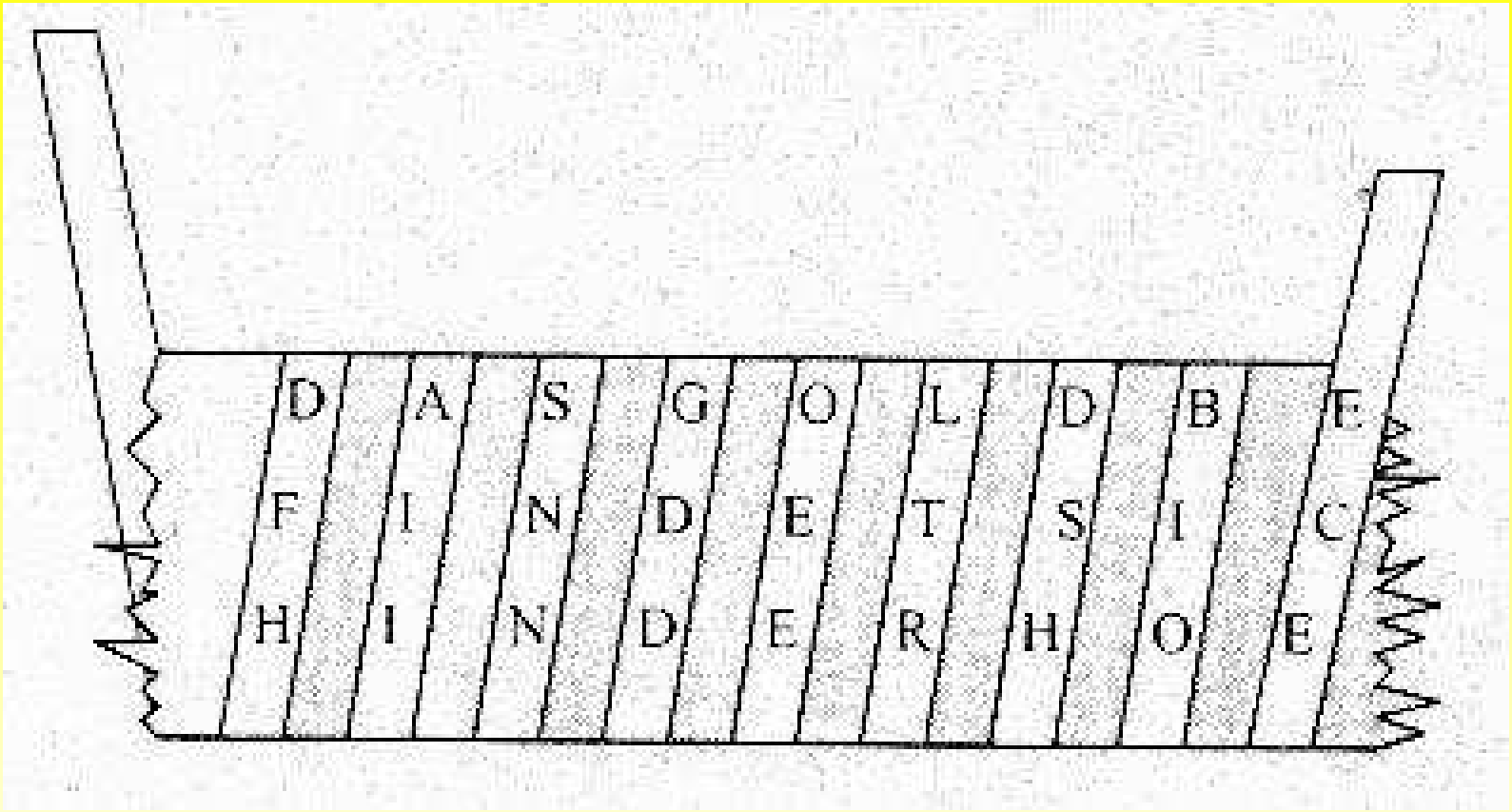
Daniel interpretierte es wie folgt:

- *Gezählt* sind Deine Tage, König Balsazar.
- *Gewogen* wurdest Du und für zu leicht befunden.
- *Geteilt* wird Dein Königreich zwischen den Medern und Persern.

Zur Belohnung erhielt Daniel purpurne Kleider, eine Goldkette und eine Anstellung als einer der drei obersten Beamten des Reichs. Belsazar wurde noch in derselben Nacht ermordet.

## 2.3 Kryptographie als Kriegswaffe (1)

- entwickelt ca. 475 v.Chr. in Sparta
- Erfindung des ersten kryptographischen Apparats, der Skytale
- ein Papierstreifen wird um den Stab gewickelt und mit der geheimen Nachricht beschrieben
- nach dem Abwickeln sind die Buchstaben vertauscht: **Transposition**
- der geheime Schlüssel ist die Stabdicke



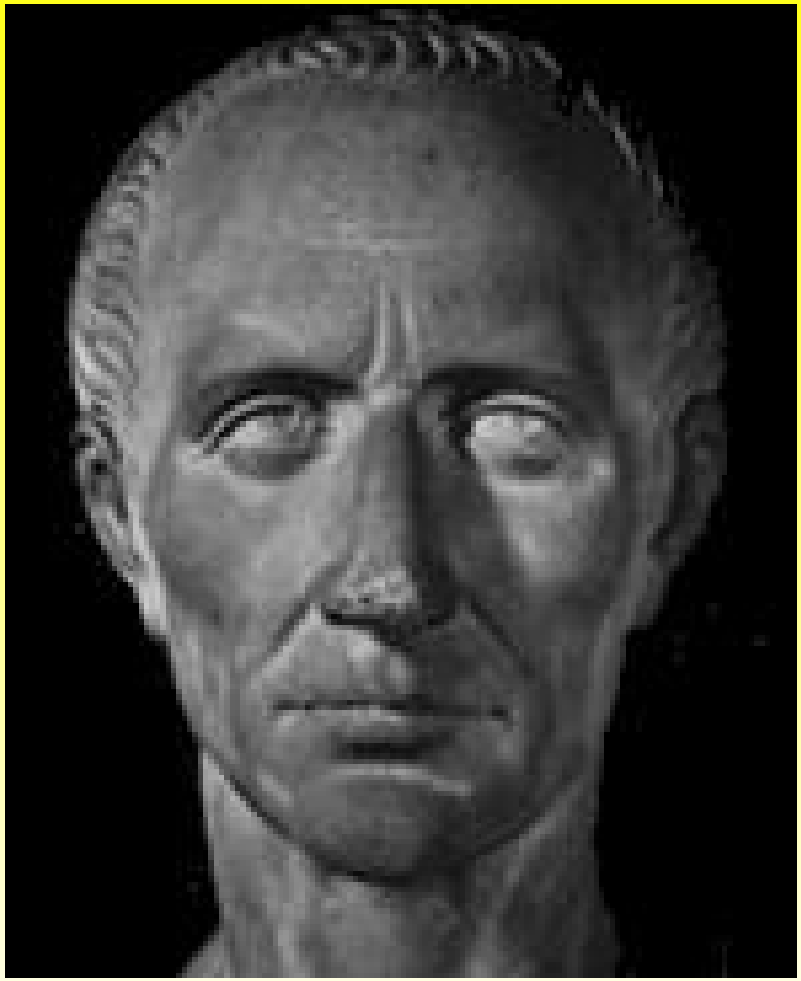

Verschlüsselte Nachricht: HFDIIANNSDDGEEORTLHSDOIBECE

## 2.4 Kryptographie als Kriegswaffe (2)

Das erste im Kriegswesen tatsächlich eingesetzte System bei dem ein Buchstabe durch einen anderen ersetzt wird **(Substitution)** stammt von einem römischen Feldherrn:

**Gaius Julius Caesar (100 – 44 v.Chr.)**

Grundprinzip der Caesar-Verschlüsselung: Ersetze jeden Buchstaben durch den im Alphabet drei Stellen später folgenden.



## Beispiel einer Caesar-Verschlüsselung

**Glh Frghnqdfnhu: jhvwhuq, khxwh, xhehuprujhq**

**Die Codeknacker: gestern, heute, uebermorgen**

- Kennt man das verwendete Kryptosystem, so ist die Caesar-Verschlüsselung extrem leicht zu knacken.
- Noch im Jahre 1915 wurde eine Caeser-Verschlüsselung in der russischen Armee eingeführt, nachdem es sich herausgestellt hatte, dass man den Offizieren etwas Komplizierteres nicht zumuten konnte.

# 3 – Drendd im Oriendd

## 3.1 Das Codeknacken in der Literatur

Die erste literarische Erwähnung des Codeknackens in einem Werk der Weltliteratur stammt von Vātsyāyana und erschien im 4. Jhd. in seinem Buch

**Kāma - sūtra**

Um für die Männer attraktiv zu sein, sollte eine Frau 64 Künste ("Yogas") kennen und regelmässig üben.

**Yogas Nr. 44/45: Mlecchita - Vikalpā**
**Codeknacken und in Geheimschrift schreiben**

## 3.2 Das erste Codeknacker-Buch

wurde ca. 850 in Baghdad veröffentlicht von

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

und hieß

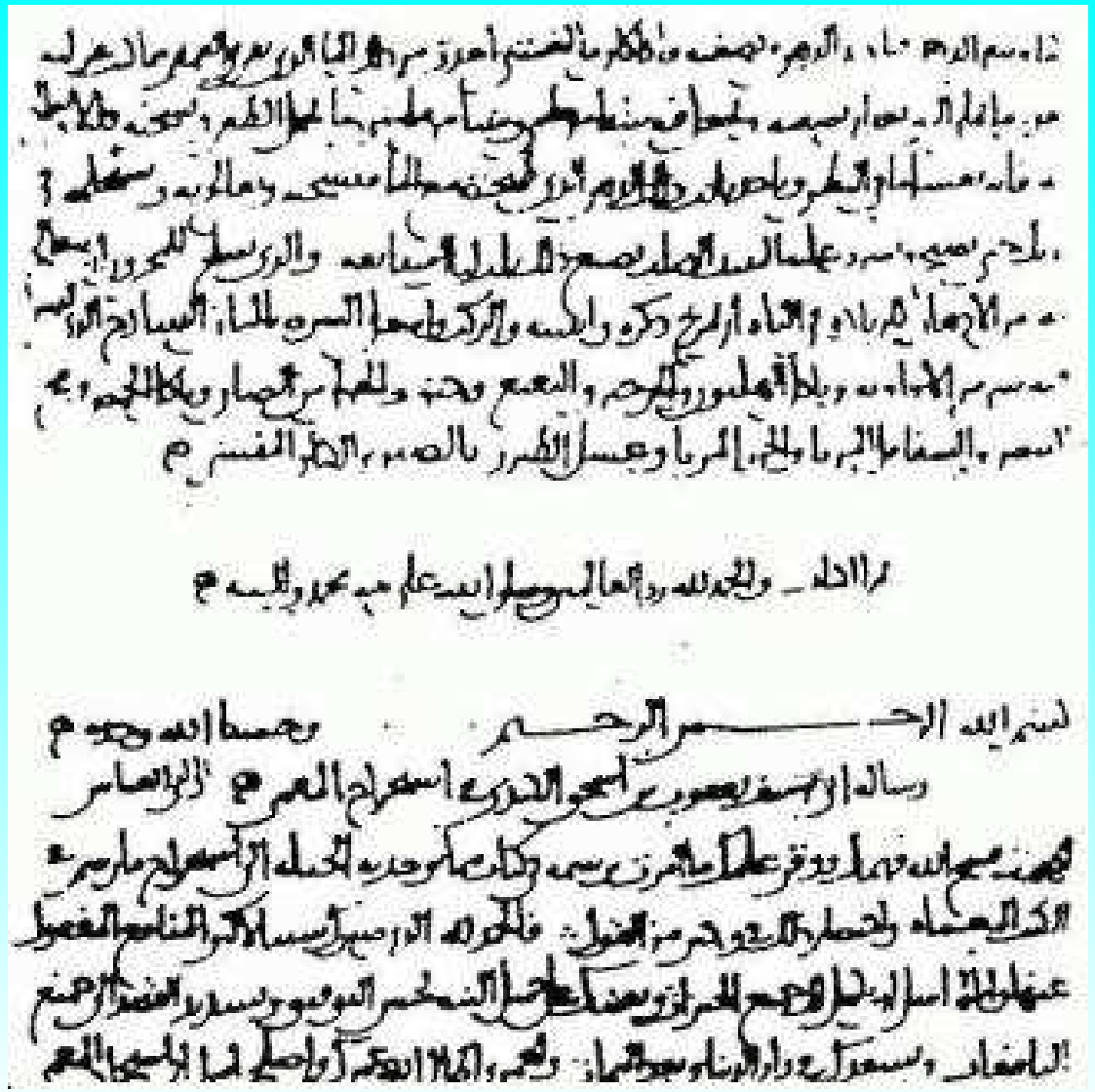
**Risalah fi Istikhraj al-Mu'amma**

Manuskript für die Entschlüsselung verschlüsselter Nachrichten

Al-Kindi war hauptberuflich Philosoph und Mathematiker am

**Haus der Weisheit**

der Kaliphen von Bagdad. Sein Buch beginnt wie folgt:




SYRIA
الجمهورية العربية السورية

## 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.

- Die Methode von Al-Kindi nennt man die **Häufigkeitsanalyse**.
- Mit ihr kann man jede **monoalphabetische** Verschlüsselung knacken, d.h. jede Verschlüsselung bei der jeder Buchstabe durch genau ein Symbol ersetzt wird.
- Die Häufigkeitsanalyse funktioniert auch, wenn Transposition und Substitution kombiniert werden, denn eine Transposition verändert die Häufigkeitsverteilung der Buchstaben nicht!
- Um eine Transposition zu knacken, kann man die Häufigkeitsanalyse verfeinern: betrachte auch die Häufigkeiten der **Digraphen** (Kombinationen von zwei Buchstaben).

Al-Kindis Buch wurde erst 1987 wiederentdeckt. Bis dahin kannte man nur die Beschreibung der verschollenen Arbeiten von

**Tāj ad-Din ‘Ali ibn ad-Duraihim ben Muhammad ath-Tha‘ālibi al-Mausili (1312-1361).**

Diese waren in der 14-bändigen Enyzklopädie aus dem Jahre 1412 enthalten, welche verfaßt wurde von

**Shihab al-Din abu ‘l‘Abbās Ahmad ben ‘Ali ben Ahmad ‘Abd Allāh al-Qalqashandi.**

# Legrand versus Captain Kidd

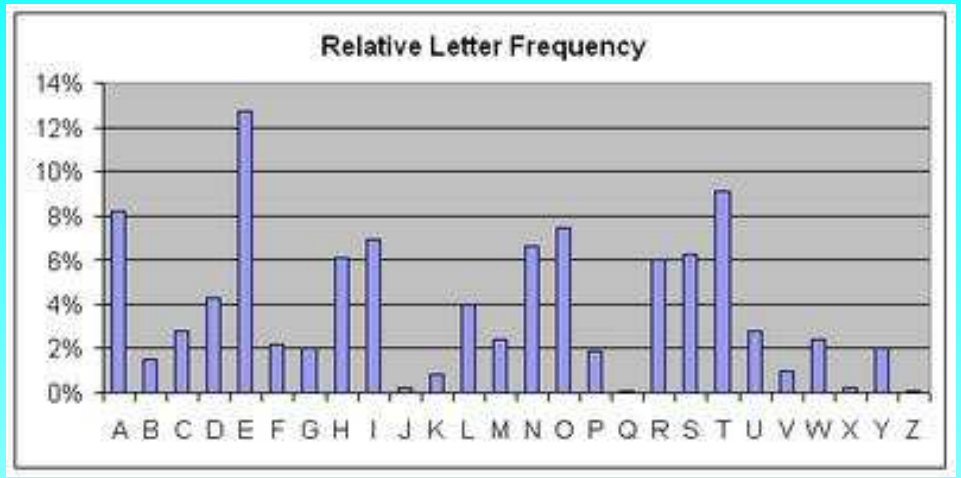
## Beispiel einer Häufigkeitsanalyse *a la* Al-Kindi

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%).

Unsere Zwischenresultat lautet jetzt:

| | | | | | | |
|---|---|---|---|---|---|---|
| 53 ≠≠ † | 305)) | *INTHE* | 2*I*)*H* ≠ | .)*H* ≠) | *TE*0*IN* | *THE*†*E* |
| ]/*I*0) | )*E*5*T*1 | ≠ *RT*:≠ | *NE*†*E*3 | *REE*)5 | *N*†*THI* | *RTEEN* |
| 9*IN*?*T* | *E*)*N*≠*R* | *THE*5) | *T*5*N* † 2 | :*N*≠*RT* | *H*95*IN* | 2*R*5*N*− |
| *H*)*E*]/ | *ENTH*0 | *I*92*E*5 | )*T*)*I*† | *E*)*H* ≠≠ | *T*1*R* ≠ 9 | *THE*0*E* |
| 1*TE*:*E* | /1*THE* | †*E*5*TH* | )*HE*5† | 52*EE*0 | *INE*1*R* | /9*THE* |
| *TREET* | *HR* ≠?3 | *HTHE*) | *H*≠*T*1*I* | 1*T* : 1*E* | *ET* ≠?*T* | |

Die letzte Zeile “tree thr...h the” macht nur für “through” Sinn, also ≠↦ $O$ (bei 7% vs. 8%) und ? ↦ $U$ (bei 1.5% vs. 3%) sowie 3 ↦ $G$ (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 ) ↦ $S$ (bei 8.5% vs. 6%). Schließlich bleibt für das “a” nur 5 ↦ $A$ 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.

# 4 – Der Pokalfight: Amateure gegen Profis!

## 4.1 Anstoss: Die Profis stürmen vor

Die ersten kryptographischen Erfindungen der westliche Welt gelangen im 14. Jahrhundert. Ihr Zweck war die

**Politische Kryptographie**

1. **1379** benötigte der Antipapst **Clemens der VII**, der nach Avignon geflohen war, ein neues Verschlüsselungssystem.
2. Sein Assistent **Gabrieli di Lavinde** erstellte eine Liste von geläufigen Wörtern zusammen mit zweibuchstabigen Ersetzungen.
3. Wörter, die nicht in der Liste enthalten waren, wurden durch eine monoalphabetische Substitution verschlüsselt.

So entstand ein Kryptosystem, das in den nächsten 550 Jahren im diplomatischen Schriftverkehr fast ausschließlich verwendet wurde:

**der Nomenklator.**

Im Laufe der Zeit wurde der Nomenklator mehrfach verbessert:

1. **1401** Der Graf von Mantua (Italien) verwendet mehrere Verschlüsselungen für häufige Vokale.
2. **ca. 1630** Erste Verwendung von Codebüchern in Spanien, um die mittlerweise über 1000 Wortersetzungen aufzulisten.
3. **ca. 1660** führt der berühmte frz. Codeknacker Antoine Rossignol das erste zweiteilige Codebuch ein: indem man die zu ersetzenden Wörter und die Codezeichen (Buchstabengruppen oder Zahlen) in zwei separaten Listen anordnet, kann man auch einen komplizierten Nomenklator effizient einsetzen.

## 4.2 Die Amateure schlagen zurück

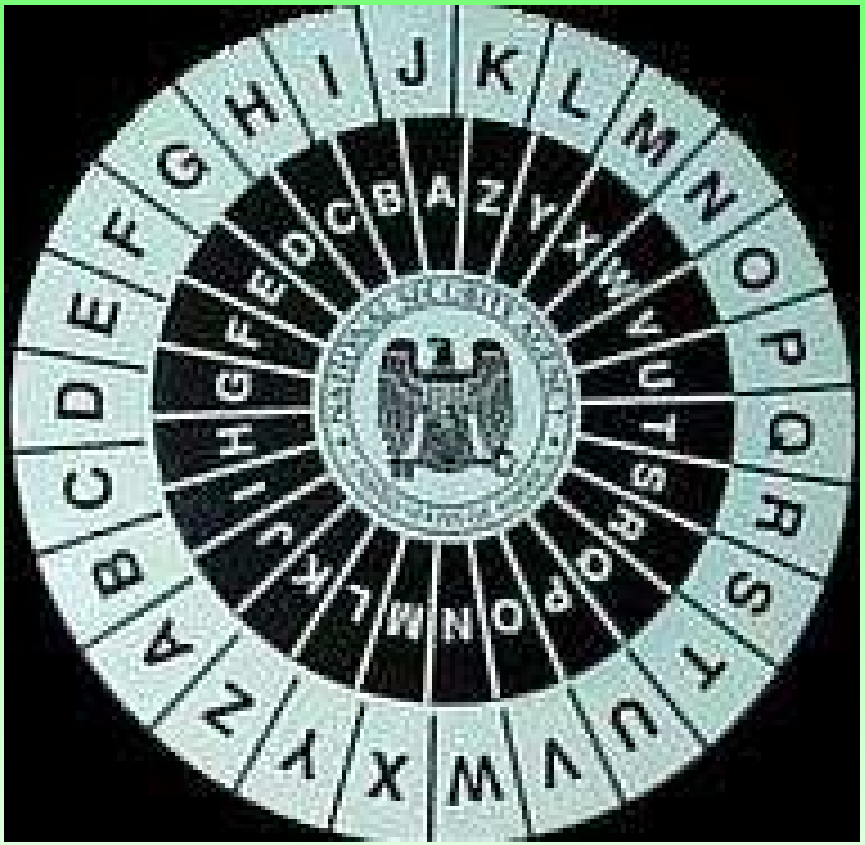
Eine der bedeutendsten kryptographischen Erfindungen der Neuzeit gelang

**Leon Battista Alberti (1404 – 1472)**

einem Universalgenie der Renaissance: Architekt, Mathematiker, Dichter, Kunsttheoretiker, Organist und Hobby - Codeknacker.

Sein Buch **De componendis cyphris** (1466) enthält die erste

**polyalphabetische Verschlüsselung**




Ein Emblem der **N**ational **S**ecurity **A**gency

## Die Alberti-Verschlüsselung

1. Bei fester Stellung der beiden Ringe ergibt sich eine Substitution.
2. Nach drei oder vier Wörtern wird die Stellung der Ringe verändert. Jede neue Ringstellung wird dem Empfänger durch einen eingefügten Großbuchstaben mitgeteilt.
3. Da derselbe Buchstabe je nach Stellung der Ringe völlig verschieden verschlüsselt wird, ist keine Häufigkeitsanalyse mehr möglich.

## Ein Beispiel

Der Text **“es steht eins zu null fuer die amateure”** soll verschlüsselt werden. Es werden folgende **Alphabete** verwendet:

| *Klartext* | *ABCDE* | *FGHIJ* | *KLMNO* | *PQRST* | *UVWXYZ* |
|---|---|---|---|---|---|
| *Stellung* 1 | *eltox* | *rinqa* | *pwcdu* | *kjbyg* | *vhsfzm* |
| *Stellung* 2 | *nqapw* | *cdukq* | *bygvh* | *sfzme* | *ltoxri* |
| *Stellung* 3 | *ygvhs* | *fzmel* | *toxri* | *nqapw* | *cdukqb* |

Wir erhalten folgenden Geheimtext:

**E xy ygxng xqdy N il vldd clwg Y hes yxywscas**

## 4.3 Die Amateure bauen ihren Vorteil aus

1. **1518** erschien das erste gedruckte Buch über das Codeknacken. Es hatte den Titel

   **Polygraphiae libri sex**

   ("Sechs Bücher über polyalphabetische Verschlüsselung", 540 Seiten) und war von dem Abt **Johannes Trithemius**.

   Trithemius verwendet für den ersten Buchstaben eine Caesar-Verschiebung um eins, für den zweiten Buchstaben eine Caesar-Verschiebung um zwei, etc.

2. **1550** beschrieb der Mailänder Arzt und Mathematiker **Girolamo Cardano** in zwei seiner **242 Bücher** eine Variation von Albertis Methode, die einen **Autoschlüssel** enthält:

   Um einen Buchstaben zu verschlüsseln, wird er selbst verwendet, um die Position der Drehscheibe zu bestimmen. Leider ist diese Methode nicht eindeutig und daher nicht entschlüsselbar!

3. **1585** schrieb **Blaise de Vigènere** das über 600-seitige Werk **Traictè des Chiffres**.

   Nachdem er als Sekretär diverser Adeliger gearbeitet hatte, ging er 1570 mit 47 Jahren in Frühpension, schenkte seine jährlichen Pensionszahlungen den Armen von Paris, heiratete ein junges Mädchen und begann Bücher zu schreiben. Als er obiges Werk schrieb, hatte er gerade eine einjährige Tochter.

Außer einer Sammlung aller bis dato bekannten Cryptosysteme enthält Vigenères Buch

- die erste europäische Darstellung japanischer Ideogramme,
- die Grundlagen von Alchemie, Magie und die Geheimnisse der Kabbalah,
- die Mysterien des Universums und ein Rezept zur Goldherstellung.

Vigenère schrieb aber nichts über das Codeknacken, sondern bezeichnete es als **nutzloses Zermartern des Gehirns**.

Überhaupt erklärte er: **“Alles in der Welt ist verschlüsselt. Die gesamte Natur besteht aus Codes und Geheimschrift.”**

Vigenère erfand das erste funktionierende polyalphabetische System mit Autoschlüssel:

- Sender und Empfänger starten mit einem vereinbarten Geheimbuchstaben zur Festlegung der ersten Stellung der Scheibe.
- Der erste Buchstabe des Klartexts gibt die Stellung der Scheibe für die Verschlüsselung des zweiten, der zweite für den dritten, u.s.w.

Obwohl Vigenères Sytem recht sicher ist, geriet es sofort in völlige Vergessenheit und wurde erst um 1890 wiedererfunden. Stattdessen wurde Vigenères Namen mit folgendem viel einfacheren und unsicheren System verknüpft:

- Wiederhole ein geheimes Schlüsselwort immer wieder.
- Der $x$-te Buchstabe dieses Bandwurms legt die Stellung der Scheibe zur Verschlüsselung des $x$-ten Klartextbuchstabens fest.

## Beispiel für eine Vigenère-Verschlüsselung

Das geheime Schlüsselwort sei **KATZE**. Es entspricht Verschiebungen des Alphabets um $(10, 0, 19, 25, 4)$ Buchstaben. Wir schreiben 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 |

Dann wenden wir diese Verschiebungen an und erhalten

| $C$ | $E$ | $G$ | $C$ | $I$ | $D$ | $B$ | $B$ | $S$ | $X$ | $O$ | $H$ | $B$ | $K$ | $J$ | $O$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Für die Codeknacker war dieses **"Vigenère Kryptosystem"** leichter überwindbar. Doch noch im Jahre **1917** wurde es in der Zeitschrift **Scientific American** als unknackbar bezeichnet!

## 4.4 Die Profis schießen ein Eigentor!

**1. Akt: 1577 – der verschossene Elfmeter**

**Maria Stuart:** jung, sehr attraktiv, mutig, streng katholisch.

Sie war aus ihrem Königreich Schottland von protestantischen Aufständischen vertrieben worden und lebte in England unter Hausarrest.

Leider auch: stur, dickköpfig und kapriziös.

**Don Juan von Österreich:** der große Sieger der Schlacht von Lepanto plant, nachdem er die Aufständischen in den Niederlanden bezwungen hat, mit einer Armee den Ärmelkanal zu überqueren, England zu erobern, Maria Stuart zu heiraten und ein katholisches Königreich zu begründen.

In mit Hilfe des spanischen Nomenklators verschlüsselten Briefen teilt er dies seinem König, Philipp II. von Spanien mit.

Die Briefe werden abgefangen, von dem brillianten flämischen Codeknacker **Philip von Marnix** entschlüsselt und den Engländern übergeben.

Als Philipp II. elf Jahre später mit seiner Grand Armada anrückt, sind die Engländer vorbereitet.

## 2. Akt: 1586 – das Drama nimmt seinen Lauf

**Anthony Babington** organisiert ein Mordkomplott gegen Königin Elisabeth. Um Marias Zustimmung zu erhalten, sendet er mit einem Nomenklator verschlüsselte Briefe.

Was beide nicht wissen ist, dass der Überbringer der Briefe ein Doppelagent im Dienste des englischen Ministers **Walsingham** ist.

Maria wünscht dem Plan in ihrer Antwort guten Erfolg und bittet um rechtzeitige Befreiung, damit sie nicht in Verdacht gerät.

Die Briefe werden sofort mit einer Häufigkeitsanalyse geknackt. Der Codeknacker **Thomas Phelippes** markiert Marias Brief mit einem Galgenzeichen.

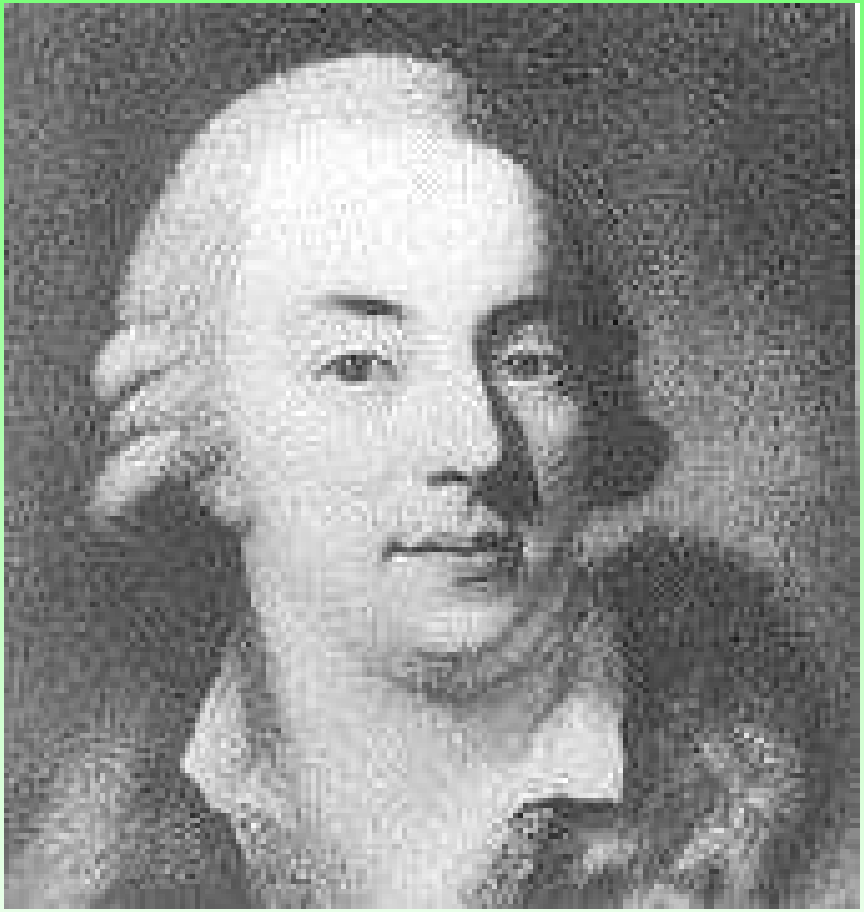
Die am Komplott Beteiligten werden gefasst. Maria Stuart wird am 7. Februar 1587 hingerichtet.

## 4.5 Auch die Amateure geraten in Bedrängnis

Etwa 200 Jahre später geraten auch polyalphabetische Verschlüsselungen unter Beschuss.

**1757** betritt ein begnadeter Physiker, Mathematiker, Lebemann und Codeknacker die Bühne:

**Jacques Casanova de Seingalt**



## 4.6 Die industriellen Codeknacker

Etwa zur gleichen Zeit wird der Nomenklator bereits systematisch und industriell geknackt. Jede Regierung hat eine eigene Abteilung mit professionellen Codeknackern, ihre

**Schwarze Kammer.**

Der Direktor der österreichischen **Geheimen Staatskanzlei** war von 1749 bis 1763

**Baron Ignaz de Koch.**

## 4.7 Noch ein Rückschlag für die Amateure

**Charles Babbage** (1791 – 1871)

- Professor für Mathematik in Cambridge
- einer der genialsten Codeknacker der viktorianischen Zeit
- Erfinder und Erbauer des ersten Computers
- verwendete als erster Algebra zum Codeknacken
- knackte bereits 1846 mit Vigenère verschlüsselte Texte
- erste Entzifferung eines "echten" Vigenère mit Autoschlüssel ca. 1854

## Die Problemchen des Herrn Babbage

- Er weigerte sich, unvollkommene Forschungen abzuschließen.
- Er publizierte fast nichts. Zum Beispiel blieb auch sein Buchplan **"The Philosophy of Decyphering"** unvollendet.
- Erst 100 Jahre später wurden seine Resultate in seinen voluminösen Aufzeichnungen entdeckt.
- Eventuell hatte er auch ein Publikationsverbot, weil England im Krimkrieg einen militärischen Vorteil erhoffte.

**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 Vigenère 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 Kunst des Codeknackens revolutioniert hatte.

## Wie knackt man einen Vigenère?

• Betrachte ein häufiges Wort oder eine Silbe, z.B. **der** oder **ung**. Ist die Distanz zwischen zwei Vorkommen von **der** durch die Länge des Schlüsselworts teilbar, so erfolgt jeweils dieselbe Verschlüsselung.

• Suche also im verschlüsselten Text nach Buchstabenkombinationen, die wiederholt vorkommen. Bestimme ihre Abstände. Der größte gemeinsame Teiler der Abstände ist ein Kandidat für die Länge $\ell$ des Schlüsselworts.

• Nimm die Buchstaben $1$, $\ell+1$, $2\,\ell+1$, $\ldots$ des verschlüsselten Texts und führe eine Häufigkeitsanalyse durch. Erhalte die erste Verschiebung, also den ersten Buchstaben des Schlüsselworts.

• Ebenso verfahre mit den Buchstaben $2$, $\ell+2$, $2\,\ell+2$, $\ldots$ des Geheimtexts, u.s.w.

Gegeben sei der Geheimtext

| | | | | |
|---|---|---|---|---|
| *HFOUL* | *WUWIY* | *HWLFF* | *SHWUH* | *YCFWP* |
| *GUDBJ* | *GELLH* | *ILCAG* | *BLPKH* | *OFVLL* |
| *VRLMR* | *UDCFV* | *LHFFO* | *USWSY* | *EGLLZ* |
| *DABRP* | *HNVNL* | *LNQKY* | *EMBMG* | *XZFVH* |
| *ICTXU* | *CIHYM* | *VWHYG* | *DYVRL* | *AYGDB* |
| *WUQLV* | *RQIYE* | *XMFVF* | *OHVFO* | *NNOZA* |
| *RKLCZ* | *FVXRH* | *EJRUA* | *YOHPG* | *OXUXR* |
| *VUUPK* | *YCPKA* | *YAGPY* | *AVAXB* | *FOAVO* |
| *AMRLU* | *CAWLL* | *RVZYI* | *RYUYO* | *LGQHY* |
| *YEIVL* | *FFOOA* | *JBHQH* | *UNJLJ* | *EYXUA* |
| *FRNYA* | *DUHGH* | *YWULW* | *ENUAY* | *AXUXQ* |
| *HYZED* | *NYJLL* | *MVFOY* | *EGHLN* | *XMARV* |
| *WYVFO* | *YEWLC* | *AIVLZ* | *DACBQ* | *LHTHT* |
| *UPKAQ* | *RUKYA* | *NVYAQ* | *LH* | |

Wir finden folgende Wiederholungen von Buchstabengruppen:

| | | | | |
|---|---|---|---|---|
| HFOUL | WUWIY | HWLFF | SHWUH | YCFWP |
| GUDBJ | GELLH | ILCAG | BLPKH | OFVLL |
| VRLMR | UDCFV | LHFFO | USWSY | EGLLZ |
| DABRP | HNVNL | LNQKY | EMBMG | XZFVH |
| ICTXU | CIHYM | VWHYG | DYVRL | AYGDB |
| WUQLV | RQIYE | XMFVF | OHVFO | NNOZA |
| RKLCZ | FVXRH | EJRUA | YOHPG | OXUXR |
| VUUPK | YCPKA | YAGPY | AVAXB | FOAVO |
| AMRLU | CAWLL | RVZYI | RYUYO | LGQHY |
| YEIVL | FFOOA | JBHQH | UNJLJ | EYXUA |
| FRNYA | DUHGH | YWULW | ENUAY | AXUXQ |
| HYZED | NYJLL | MVFOY | EGHLN | XMARV |
| WYVFO | YEWLC | AIVLZ | DACBQ | LHTHT |
| UPKAQ | RUKYA | NVYAQ | LH | |

Diese Wiederholungen haben die folgenden Abstände:

| | | | | |
|---|---|---|---|---|
| **VFOYE** | Abstand | 16 | = | $2 \cdot 2 \cdot 2 \cdot 2$ |
| **LZDA** | Abstand | 240 | = | $2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$ |
| **QHY** | Abstand | 52 | = | $2 \cdot 2 \cdot 13$ |
| **PKA** | Abstand | 144 | = | $2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$ |
| **LFF** | Abstand | 217 | = | $7 \cdot 31$ |

Die wahrscheinlichste Schlüsselwortlänge ist also $\mathbf{2 \cdot 2 = 4}$.

Die Häufigkeitsverteilung der Buchstaben 1, 5, 9, 13, ... ist

L (19,8%)  A (10,5%)  U (9,3%)  Y (9,3%)  etc.

Also entspricht **L** wahrscheinlich dem **E** und die erste Verschiebung ist um 7 Buchstaben.

Die Häufigkeitsverteilung der Buchstaben 2, 6, 10, 14, ... liefert Y mit 22,1% als wahrscheinliche Entsprechung des **E** und die zweite Verschiebung ist um 20 Buchstaben.

Die Häufigkeitsverteilung der Buchstaben 3, 7, 11, 15, ... liefert R mit 14,1% als wahrscheinliche Entsprechung des **E** und die dritte Verschiebung ist um 13 Buchstaben.

Die Häufigkeitsverteilung der Buchstaben 4, 8, 12, 16, ... liefert H mit 11,8% als wahrscheinliche Entsprechung des **E** und die vierte Verschiebung ist um 3 Buchstaben.

Insgesamt haben wir die Verschiebungen $(7, 20, 13, 3)$ und das geheime Schlüsselwort ist **HUND**.

Jetzte können wir den Geheimtext vollständig knacken. Es ergibt sich:

| | | | | |
|---|---|---|---|---|
| *ALBRE* | *CHTBE* | *UTELS* | *PACHE* | *RISTI* |
| *MHAUP* | *TBERU* | *FEIND* | *URCHA* | *USSER* |
| *IOESE* | *RWISS* | *ENSCH* | *AFTLE* | *RDERM* |
| *ATHEM* | *ATIKE* | *RANDE* | *RJUST* | *USLIE* |
| *BIGUN* | *IVERS* | *ITAET* | *ARBEI* | *TATAU* |
| *CHNEB* | *ENBER* | *UFLIC* | *HNICH* | *TALSG* |
| *EHEIM* | *CODEE* | *XPERT* | *EBEIM* | *BUNDE* |
| *SNACH* | *RICHT* | *ENDIE* | *NSTDO* | *CHGIL* |
| *TSEIN* | *INTER* | *ESSEV* | *ORALL* | *EMDER* |
| *ERFOR* | *SCHUN* | *GUNDE* | *NTWIC* | *KLUNG* |
| *SOGEN* | *ANNTE* | *RCHIP* | *KARTE* | *NUNDD* |
| *ERFRA* | *GEWIE* | *SICHE* | *RDARA* | *UFGES* |
| *PEICH* | *ERTEI* | *NFORM* | *ATION* | *ENGEM* |
| *ACHTW* | *ERDEN* | *KOENN* | *EN* | |

Nun brauchen wir nur noch die Interpunktion hinzuzufügen:

Alfred Beutelspacher ist im Hauptberuf ein durchaus seriöser Wissenschaftler. Der Mathematiker an der Justus Liebig Universität arbeitet auch nebenberuflich nicht als Geheimcodeexperte beim Bundesnachrichtendienst, doch gilt sein Interesse vor allem der Erforschung und Entwicklung sogenannter Chipkarten und der Frage, wie sicher darauf gespeicherte Informationen gemacht werden können.

(Quelle: FAZ, 15.2.1995)

## 4.8 Der Untergang der Profis

**Vorspiel: Der Untergang der Magdeburg**

**1.8.1914:** Deutschland erklärt Russland den Krieg.

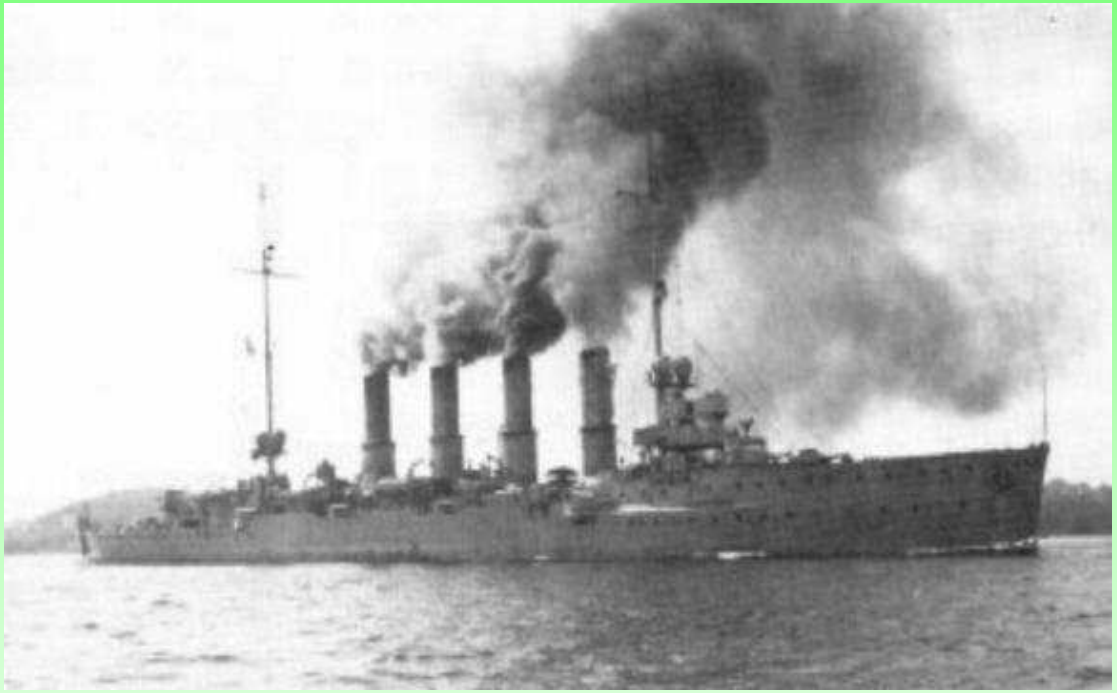
**25.8.1914:** Der deutsche kleine Kreuzer "Magdeburg" läuft am finnischen Meerbusen auf Grund.

**26.8.1914:** Eines der drei Signalbücher an Bord wird verbrannt.

**Sept. 1914:** Russische Matrosen und Taucher finden im Schiff und am Meeresgrund die beiden anderen Signalbücher.

**13.10.1914:** Die Engländer erhalten die Codebücher.

**Nov. 1914:** Die Codeknacker im englischen **Room 40** lesen die Funksprüche der deutschen Marine: der einteilige Nomenklator wurde mit einer monoalphabetischen Substitution nachververschlüsselt.



**Der kleine Kreuzer Magdeburg**

| Zahlen- Signal | Buchstaben- Signal | | | Bedeutung |
|---|---|---|---|---|
| 534 27 | C | a | E | Bodenanstrich |
| 28 | C | a | F | Bodenbeplattung |
| 29 | C | a | G | Bodenbeschaffenheit |
| 534 30 | C | a | H | Bodenbeschlag |
| 31 | C | a | Î | Bodenstück |
| 32 | C | a | J | Bodenventil (Nr. n) |
| 33 | C | a | K | Bodenverschluß ⊣ |
| 34 | C | a | L | Bodenzünder |
| 35 | C | a | M | Bö ig |
| 36 | C | a | N | Bogen |
| 37 | C | a | O | bogenförmig |
| 38 | C | a | Ō | Bogenlampe |
| 39 | C | a | P | Bohle |
| 534 40 | C | a | Q | Bohne (n kg) |
| 41 | C | a | R | bohren ung, Bohr- *[s. Grund]* |
| 42 | C | a | S | Bohrer |
| 43 | C | a | T | Boje, Bojen- *[s. Anker, Kohlen, Leine]* |
| 44 | C | a | U | Boje auf den Anker stecken |
| 45 | C | a | Ū | Boje aufnehmen (fischen) |
| 46 | C | a | V | Boje auslegen |
| 47 | C | a | W | Boje beleuchten |
| 48 | C | a | X | Boje über Bord |
| 49 | C | a | Y | eine Boje über Bord werfen und wieder fischen |
| 534 50 | C | a | Z | an der Boje festmachen |
| 51 | C | a | γ | an die Boje gehen |
| 52 | C | γ | A | Boje falsch hinlegen |
| 53 | C | γ | Ā | Boje legen |

## Zweiter Akt: Der totale U-Boot Krieg

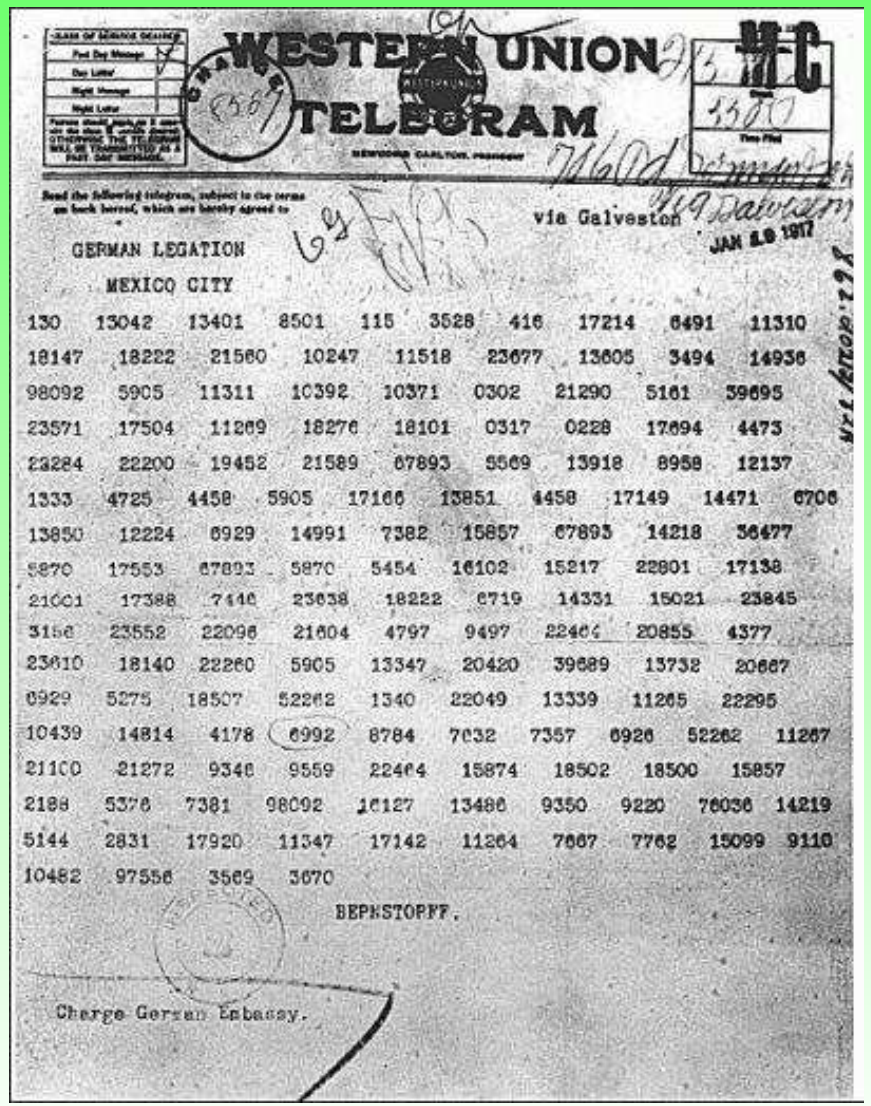
**Dez. 1916:** Um England zu besiegen, plant Deutschland seine U-Boote auch einzusetzen, um die Nachschubschiffe der neutralen USA mit Kurs auf England zu zerstören.

**16.1.1917:** Außenminister Zimmermann sendet ein verschlüsseltes Telegramm nach Mexiko, das die deutschen Pläne offenbart: der Kriegseintritt der USA soll verhindert werden, indem sie in einen Zweifrontenkrieg gegen Mexiko und Japan verwickelt werden.

**1.2.1917:** Beginn des totalen U-Boot Kriegs

**5.2.1917:** **Room 40** hatte des Telegramm entschlüsselt. Der verwendete Code 13040 ähnelte denen im Signalbuch der Magdeburg.

**22.2.1917:** Die Engländer spielen das Telegramm den USA zu.



WESTERN UNION TELEGRAM

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
9870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

## Endspiel: Der totale Untergang

**1.3.1917:** Das Zimmermann-Telegramm wird in der New York Times veröffentlicht.

**6.4.1917:** Die USA erklären Deutschland den Krieg.

**Nov. 1919:** Deutschland und Österreich/Ungarn kapitulieren.

## Nachwort: Das einzig sichere Kryptosystem

**17.12.1917:** Gilbert S. Vernam entwickelt den One Time Pad: die digitalisierte Nachricht und eine zufällige 0/1-Folge werden binär addiert. Zum Entschlüsseln benötigt man dieselbe 0/1-Folge. Der Schlüssel ist also so lange wie die Nachricht und daher unhandlich.

Der One Time Pad ist das einzige Kryptosystem dessen Sicherheit mathematisch beweisbar ist.

# 5 – Hypermoderne Kryptoanalysten

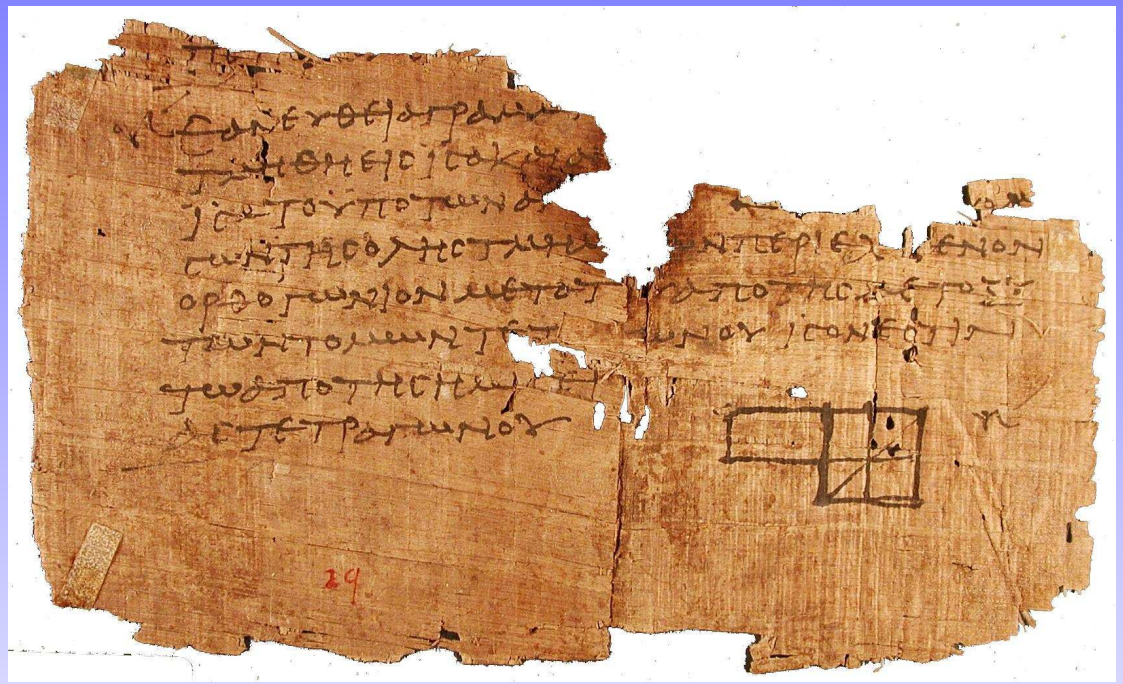
## 5.1 Noch mehr Definitionen

**Definition.** Eine Zahl $> 1$ heisst **Primzahl**, wenn sie nur durch 1 und sich selbst teilbar ist.

**Satz.** Ist ein Produkt von zwei Zahlen durch eine Primzahl teilbar, so ist bereits eine der beiden Zahlen durch diese Primzahl teilbar.

**Beweis:** Siehe **Euklid**, Die Elemente, Band VII, Satz 30 (erschienen in Alexandria, ca. 300 v.Chr., $>$ 1000 Auflagen)

**Definition.** Teilt man eine Zahl $a$ durch eine Zahl $b$, so bezeichnen wir den Divisionsrest mit **a mod b** (sprich **"a modulo b"**).



Eine Seite aus Band II der Elemente

**Satz. (Der kleine Satz von Fermat)**

Sei $p$ eine Primzahl und $a$ eine nicht durch $p$ teilbare Zahl. Dann gilt

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

**1640:** Behauptung ohne Beweis durch **Pierre de Fermat**

**1683:** erster Beweis durch **Gottfried Wilhelm Leibnitz**

**1760:** Beweis einer Verallgemeinerung durch **Leonhard Euler**

Ist eine Zahl $n$ Produkt zweier verschiedener Primzahlen $p$ und $q$, so gilt für jede zu $n$ teilerfremde Zahl $a$ die Formel

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

# Fermat – Leibnitz – Euler

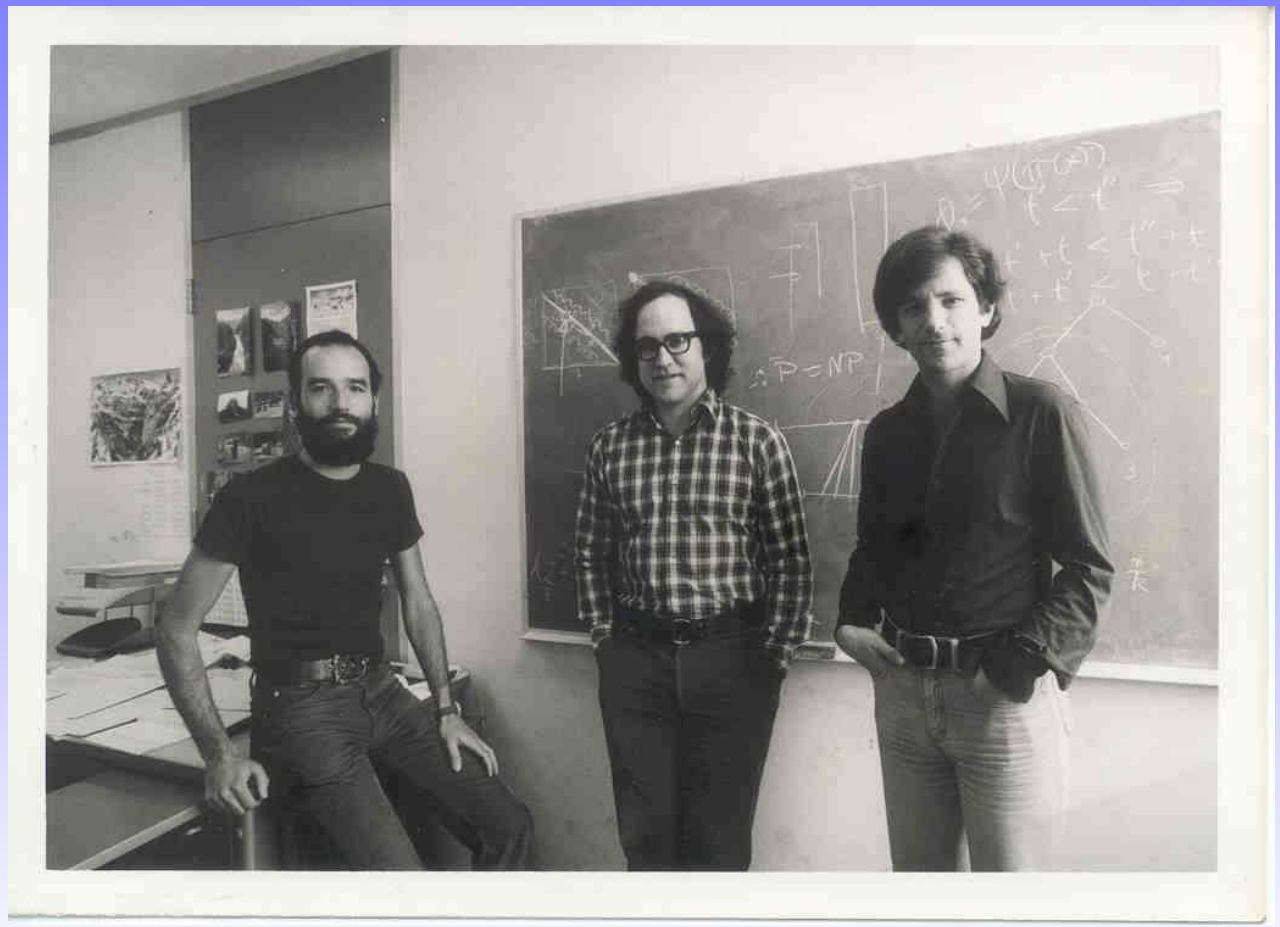


## 5.2 Das RSA Kryptosystem

### Was bedeutet RSA ?

**R**epublik **S**üd-**A**frika

# Rivest – Shamir – Adleman



## Mamma Mia! Drei Väter – eine schwere Geburt!

**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."**

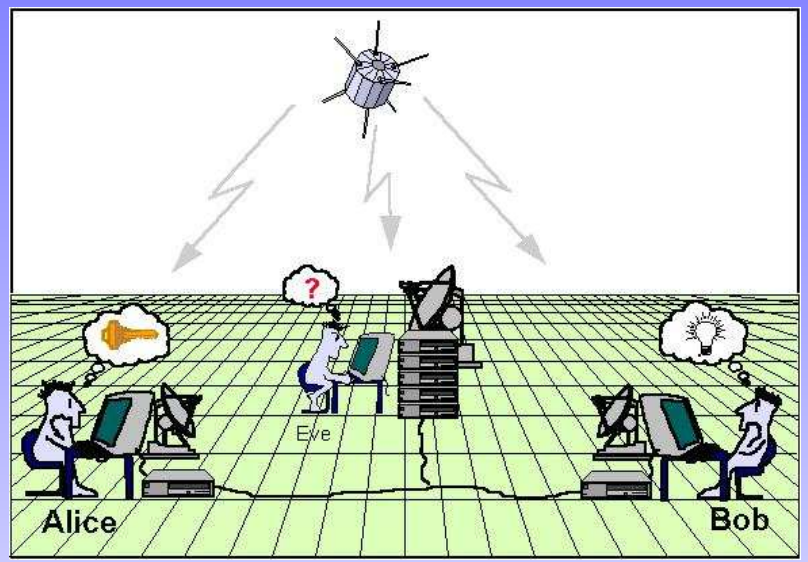
**Feb. 1978:** Der Artikel "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" erscheint in *Communications of the ACM*, Band 21, Seiten 120-126.

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.

## Ist RSA wirklich sicher?

**Im Prinzip ja, sprach Radio Eriwan.**

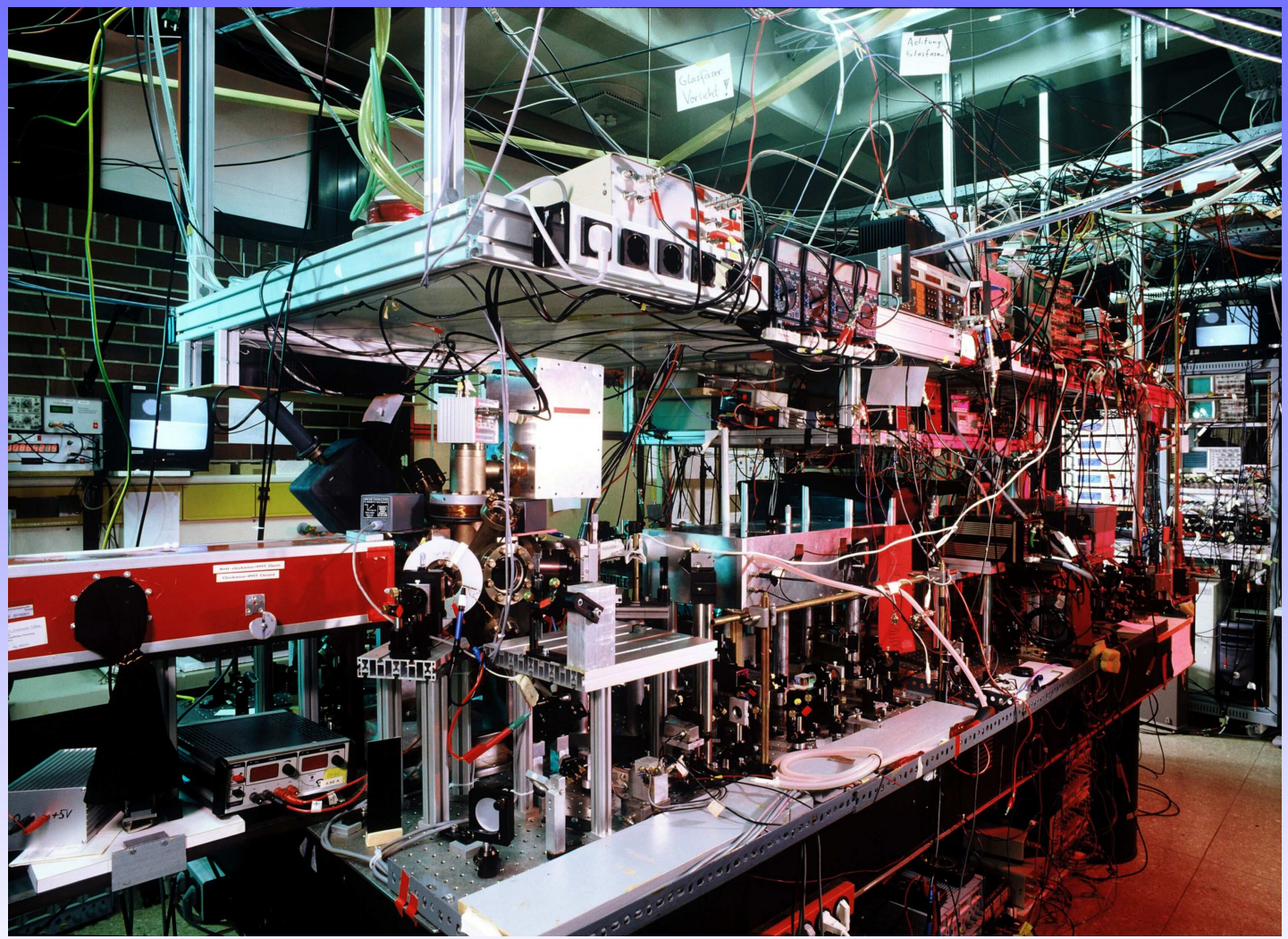
Selbst mit modernsten Computern und den besten bekannten Algorithmen kann man Zahlen $n$ nicht in ihre Faktoren $p$ und $q$ zerlegen, wenn $p$ und $q$ mehr als 100 Stellen haben.

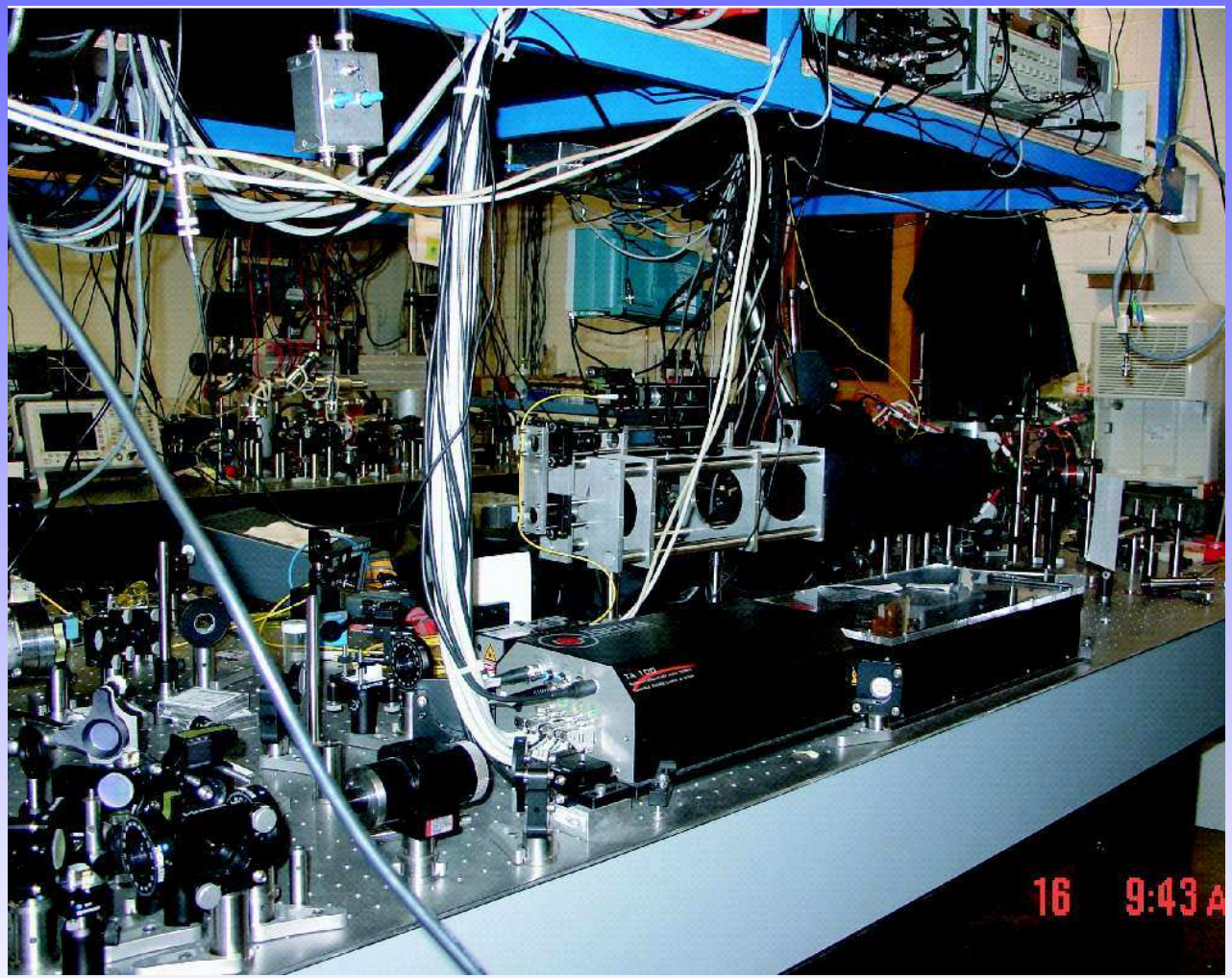
Es wurde aber trotz intensiver Bemühungen noch nicht **bewiesen**, dass die Aufgabe nicht in vernünftiger Zeit lösbar ist.

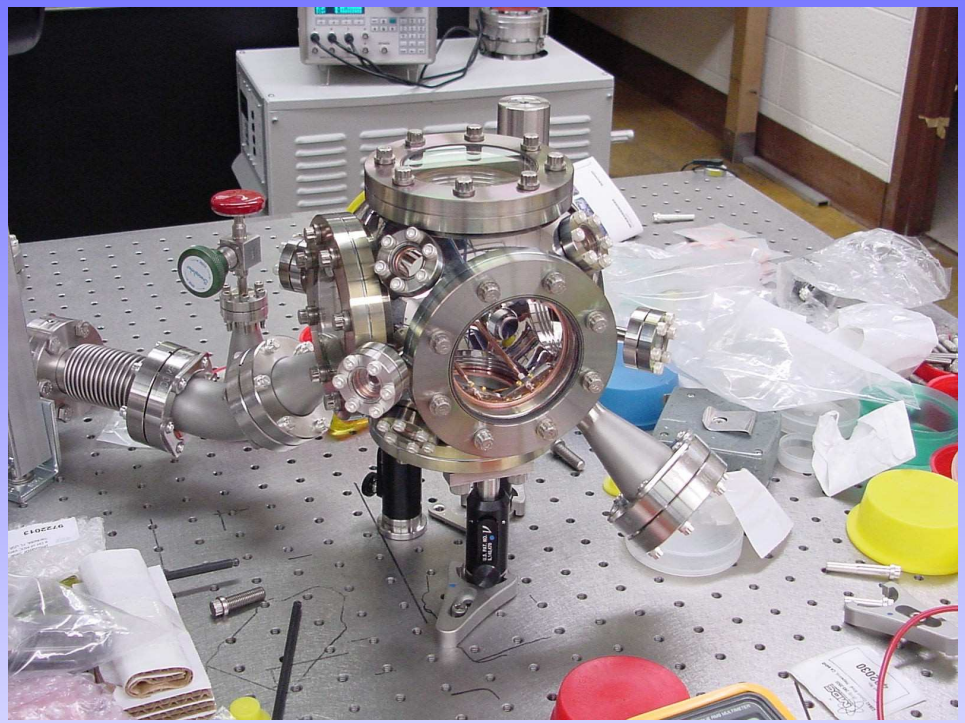
Stattdessen haben die Mathematiker bewiesen, dass man große Zahlen mit einem Quantencomputer ruck-zuck faktorisieren kann.

**Es ist also nur noch eine Frage der Zeit, bis die Codeknacker wieder einmal triumphieren!**

**Über 90% aller heute eingesetzten Kryptoverfahren verwenden RSA!**

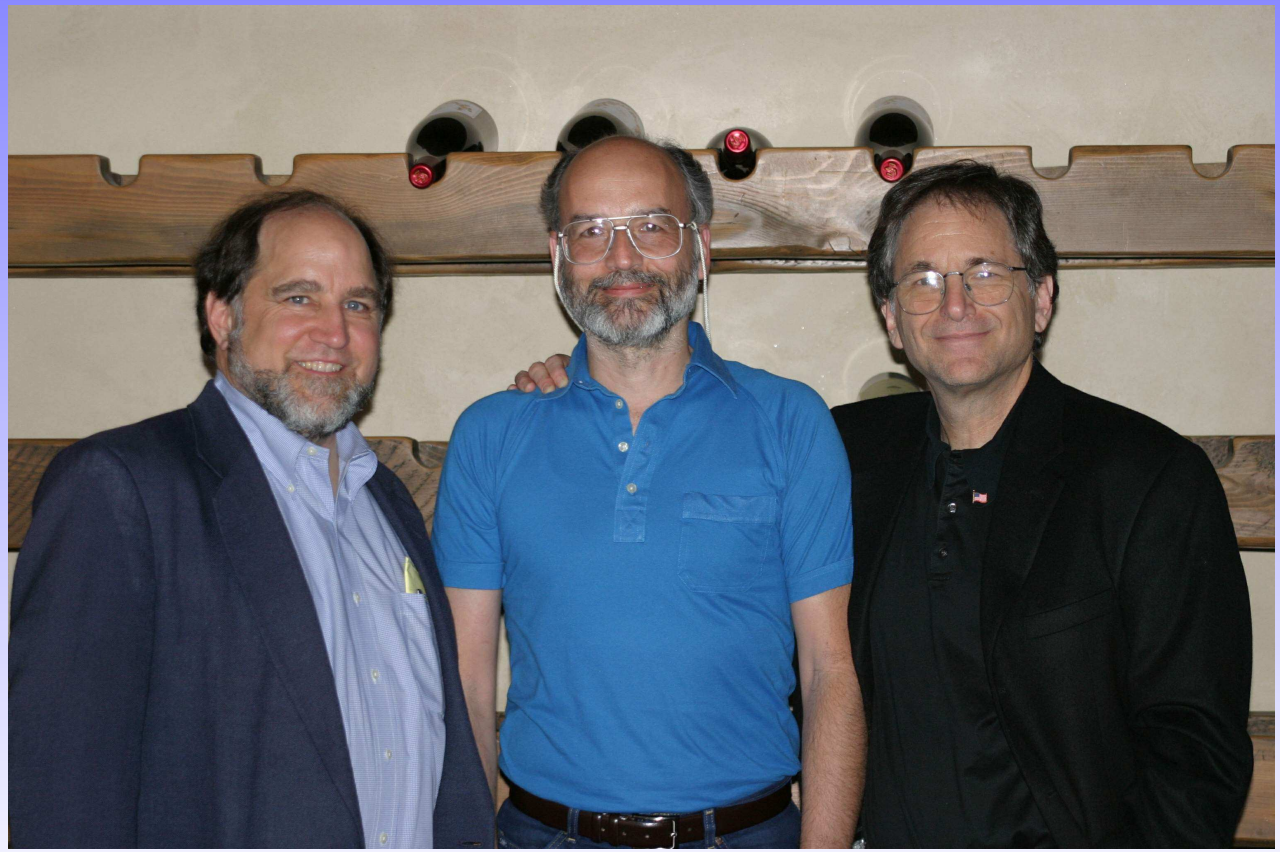



16 9:43 A



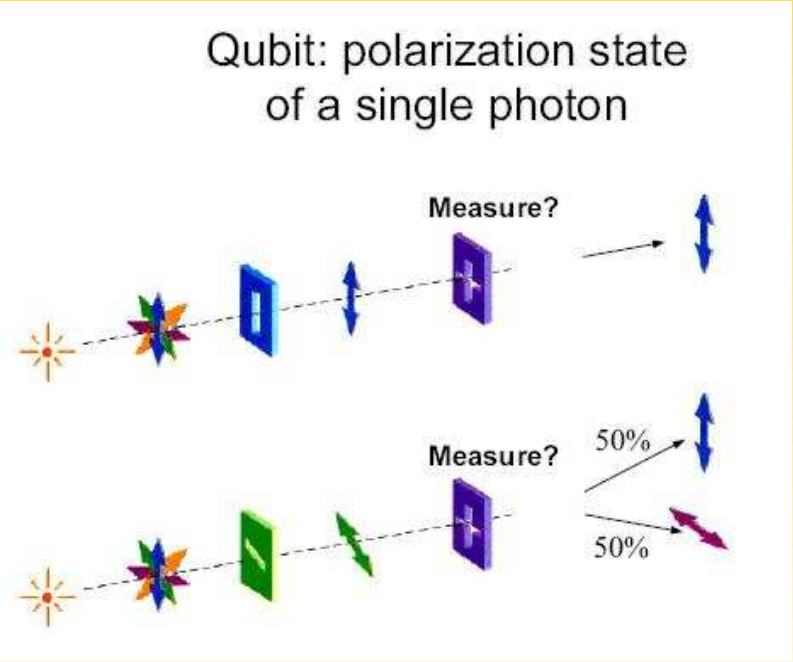
In der Zukunft könnten Computer vielleicht einmal weniger als $1,5\,t$ wiegen. (Popular Mechanics, 1949)

# Und wie sieht RSA heute aus?



# 6 – Und wenn sie noch nicht gestorben sind ...

## 6.1 Kann die Physik die Menschheit retten?




Grundprinzip der **Quantenkryptographie**

## Und wie soll das funktionieren?

- Es werden polarisierte Photonen übertragen, d.h. das Licht schwingt nur in eine Richtung.
- Um eine 0/1-Folge zu senden, kann Alice entweder horizontal/vertikal polarisierte Photonen (Schema $+$) oder diagonal polarisierte Photonen senden (Schema $\times$).
- Alice sendet eine lange Serie von Photonen, die in zufälligen Richtungen schwingen.
- Bob ordnet seine Meßfilter zufällig entweder in $+$ oder in $\times$ Richtung an. Er misst nur die Hälfte der Photonen korrekt.

• Alice teilt Bob öffentlich die Polarisationsschemata mit, die sie verwendet hat, aber nicht die gesendeten Bitwerte.

• Bob teilt Alice öffentlich mit, welche Bits er korrekt gelesen hat.

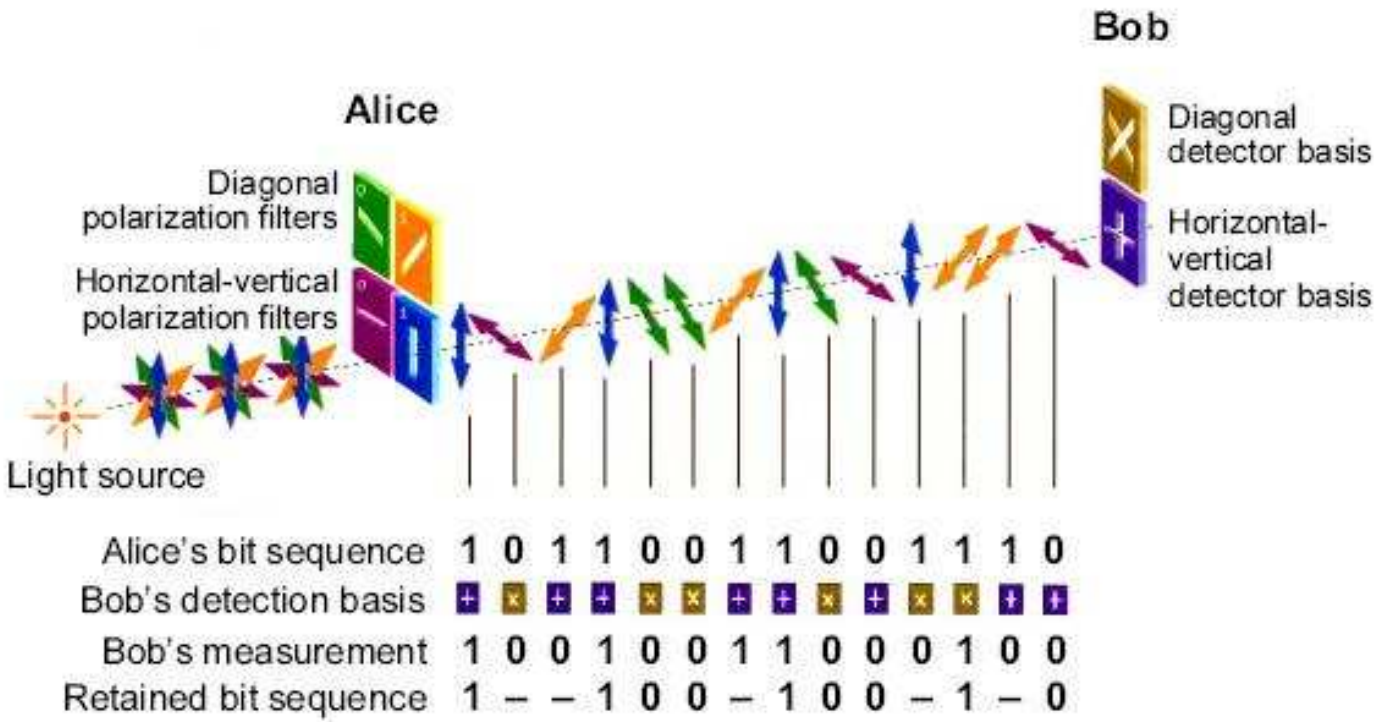
Diese bilden einen gemeinsamen geheimen Schlüssel, also ein One-Time-Pad.

• Mißt Eve unterwegs ein Photon korrekt, so bleibt dies unbemerkt. Verwendet sie aber das falsche Schema für den Meßfilter, so zerstört sie die Polarisation des Photons unwiederbringlich.

Die Sicherheit der Quantenkryptographie folgt somit aus der Quantenphysik, genauer der

**Heisenbergschen Unschärferelation.**

# Quantum key distribution



## Die Zeittafel der Quantenkryptographie

**1989:** Erstes erfolgreiches Experiment, Übertragungsstrecke **30 cm**

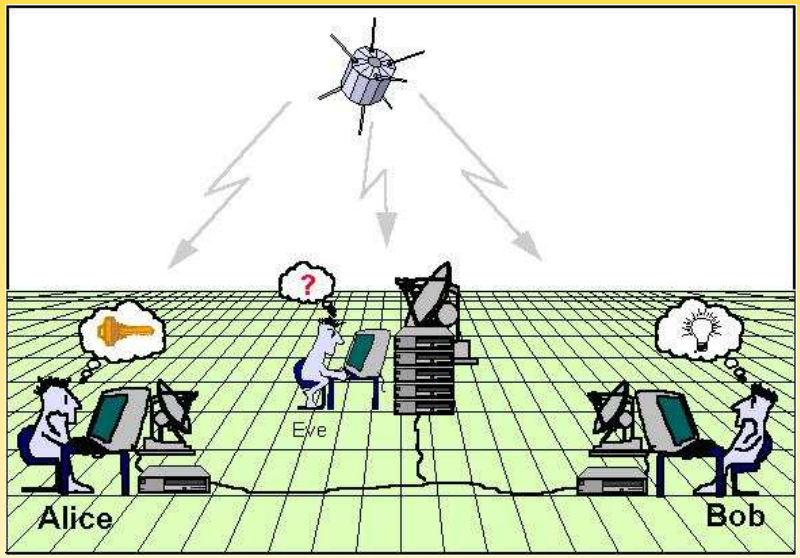
**2003:** Zwei Firmen bieten erste kommerzielle Produkte an.

**2004:** Die Firma NEC (Tokio) überträgt einen quantenkryptographischen Schlüssel über **150 km**.

**2005:** Bereits vier Firmen verkaufen Quantenkryptosysteme, Preis: ab ca. 70,000 Dollar

$>$ **2006:** `Vorhersagen sind schwierig, besonders wenn sie die Zukunft betreffen.` (Niels Bohr)

## 6.2 Kann die Informatik die Menschheit retten?




Versuchsaufbau der **informationstheoretischen Kryptographie**

## Und wie soll das funktionieren?

- Ein Satellit sendet große Mengen an Zufallsbits (0/1-Folge).
- Alice und Bob erzeugen aus diesem Datenstrom mit Hilfe einer öffentlichen Diskussion einen gemeinsamen geheimen Schlüssel.
- Eve empfängt den Datenstrom auch, kann ihn aber nicht komplett aufzeichnen. Sie kann aus der Kommunikation zwischen Alice und Bob keine Information gewinnen.
- Die Sicherheit des Verfahrens beruht auf der **Shannonschen Informationstheorie.**
- Sein Nachteil ist, dass der Satellit riesige Datenmengen aussenden muss. Auch Alice und Bob müssen große Datenmengen austauschen.

## Und wie soll das genau gehen?

**Phase I "Advantage Distillation":** Alice und Bob entnehmen dem Datenstrom nach einer vereinbarten geheimen Strategie eine geeignete Zahl von Bits. Da Eve nicht den gesamten Datenstrom protokollieren kann, haben sie einen Vorteil.

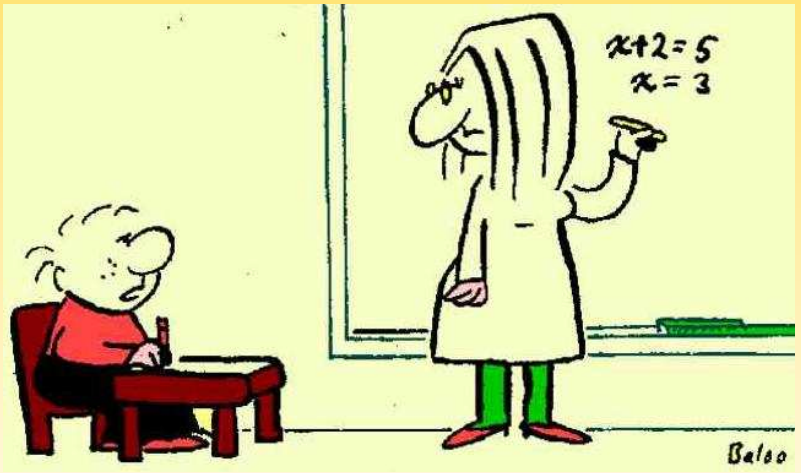
**Phase II "Information Reconciliation":** Die geheimen Schlüssel von Alice und Bob können sich durch Übertragungsfehler noch unterscheiden. Indem sie Prüfsummen ihrer Schlüssel austauschen, können sie sie angleichen, ohne viel Information an Eve zu liefern.

**Phase III "Privacy Amplification":** Mit Hilfe sogenannter universeller Hash-Funktionen können Alice und Bob den Anteil der Bits ihres Schlüssels, den Eve kennen kann, beliebig klein machen.

## 6.3 Kann die Mathematik die Menschheit retten?

### Algebraische Kryptographie

In der Algebra gibt es Rechenaufgaben, die **viel schwieriger** sind als die Zerlegung von Zahlen in Primfaktoren.




Aber gestern sagten Sie, **x** sei **zwei**!

## Das Wortproblem in Gruppen

Dieses Problem ist im Allgemeinen algorithmisch **unlösbar**.

Gegeben sei ein endliches Alphabet, z.B. $A, B, \ldots, Z$.

Wir bilden alle Wörter, z.B. $AFFE, BAUM, BANANE$.

Es werden gewisse **Relationen** eingeführt, z.B. $BA = ATRI$ oder $AN = OHN$.

Nun kann man Wörter durch die **erzeugten Relationen** abändern, z.B. $BAUM = ATRIUM$ oder
$BANANE = ATRINANE = BOHNOHNE$.

Die Frage, ob man zwei Wörter durch wiederholtes Anwenden der erzeugten Relationen ineinander überführen kann, nennt man das **Wortproblem**.

Das **Wortproblem** und das ähnlich gelagerte **Konjugatorsuchproblem** sind als Grundlage für **gruppentheoretische Kryptosysteme** vorgeschlagen worden.

Es gibt aber noch einige Probleme zu lösen:

- Man muss genügend Beispiele konstruieren, für die das Problem nachweislich schwierig ist. (Banken brauchen mindestens 1,000,000,000 Beispiele.)
- Für die bisher untersuchten Fälle gelang noch kein Nachweis, dass die Codeknacker wirklich chancenlos sind.

## Die Computeralgebra rettet die Menschheit!

Ein **Polynom** ist ein Ausdruck der Form

$$3\,x^3 + 5\,x\,y - 4\,y\,z^2 + x\,y\,z - 100.$$

Sind Polynome $f_1, \ldots, f_s$ gegeben, so bilden alle Kombinationen $f_1 \cdot g_1 + \cdots + f_s \cdot g_s$ mit Polynomen $g_1, \ldots, g_s$ ein **Polynomideal**.

Die gegebenen Polynome $f_1, \ldots, f_s$ nennt man ein **Erzeugendensystem** des Polynomideals.

Eine **Gröbner-Basis** ist ein spezielles Erzeugendensystem desselben Polynomideals mit gewissen guten Zusatzeigenschaften.

Die Berechnung einer Gröbner-Basis ist **EXPSPACE**-schwer, d.h. der benötigte Speicherplatz nimmt mit der Größe der Ausgangspolynome $f_1, \ldots, f_s$ exponentiell zu.

**Gröbner-Basis Kryptosysteme** verwenden als öffentlichen Schlüssel die Polynome $f_1, \ldots, f_s$ und als geheimen Schlüssel eine Gröbner-Basis des erzeugten Polynomideals.

Man kann auch das Wortproblem und viele andere schwierige Probleme der Algebra als Berechnungen von Gröbner-Basen formulieren.

**Bisher sind diese Probleme auch mit einem Quantencomputer nicht zu knacken!**

# Bibliographie


1. David Kahn, *The Codebreakers*, Scribner, New York 1996, 1181 Seiten

2. Simon Singh, *Codes: Die Kunst der Verschlüsselung*, dtv 2004.

3. Simon Singh, *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, dtv 2001.

4. Rolf Kippenhahn, *Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte*, Rowohlt, Hamburg 1999