§1 Geschichtlicher Überblick

Quelle. Wikipedia

Eine Skytale.

Lassen Sie sich nichts vormachen!

Beginn ?

Wann beginnt Kryptologie als systematisches Studium?

Antwort nach heutigem Wissenstand:

Im arabischen / islamischen Mittelalter.

Im 9. Jahrhundert schreibt al-Kindi eine Abhandlung über Kryptographie.

Weitere Texte im 13., 14. Jahrhundert.

Aber: Anwendung zweifelhaft.

Wörter “Ziffer”, “Chiffre”, “cipher” kommen aus dem Arabischen.

Erste verbreitete Anwendung: in der Renaissance.

Literatur

David Kahn. The codebreakers (1968, 1996)

Klaus Schmeh. Codeknacker und Codemacher (2014)

Grobeinteilung

Drei Perioden

- Bis ca. 1918. Papier- und Bleistift-Periode
- 1918 - ca. 1970. Periode der elektrisch-mechanischen Chiffriermaschinen
- Ab ca. 1970. Das elektronische Zeitalter

Die Papier- und Bleistift-Periode

Anfänge

Erste nicht-sporadische Anwendung in der Renaissance ab ca. 1450.

Verwendung von Codebüchern und Polysubstitution

ca. 1466. Leon Battista Alberti: De Componendis Cifris

Chiffrierscheibe aus der Zeit Ludwig XIV (1638 - 1715)
Quelle. Nicolas Gessler Sammlung

Verfahren mit Chiffrierscheibe ohne Umordnung und mit Codewort bekannnt unter Vigenère-Verfahren

Erster Höhepunkt

Kryptographie und -analyse haben große Bedeutung im 17. und 18. Jahrhundert (“Cabinet Noir”, Schwarze Kammer)

Es werden sogenannte Nomenclatoren benutzt. (Namen und Silben werden ersetzt.)

Ein Rätsel

Der bekannteste französische Kryptologe zur Zeit Ludwig XIV hieß Antoine Rossignol.

Rossignol heißt auf Deutsch u.a. Nachtigal. Es bedeutet auch Dietrich.

In der englischen Wikipedia findet man unter “Rossignols”:

> *The family name meant “nightingale” in French. As early as 1406 the word rossignol has served as the French term for “skeleton key” or for any tool which opens that which is locked.*

(Elektrischer) Telegraph

1833. Carl Friedrich Gauß & Wilhelm Weber (1 km)
ca. 1833. Samuel Morse
1839. Charles Wheatstone (Zeigertelegraph)
1846. August Kramer
1848. Werner Siemens

Quelle.
Denis Apel
flyingpixel.de
Wikipedia

Das Kerckhoffs'sche Prinzip

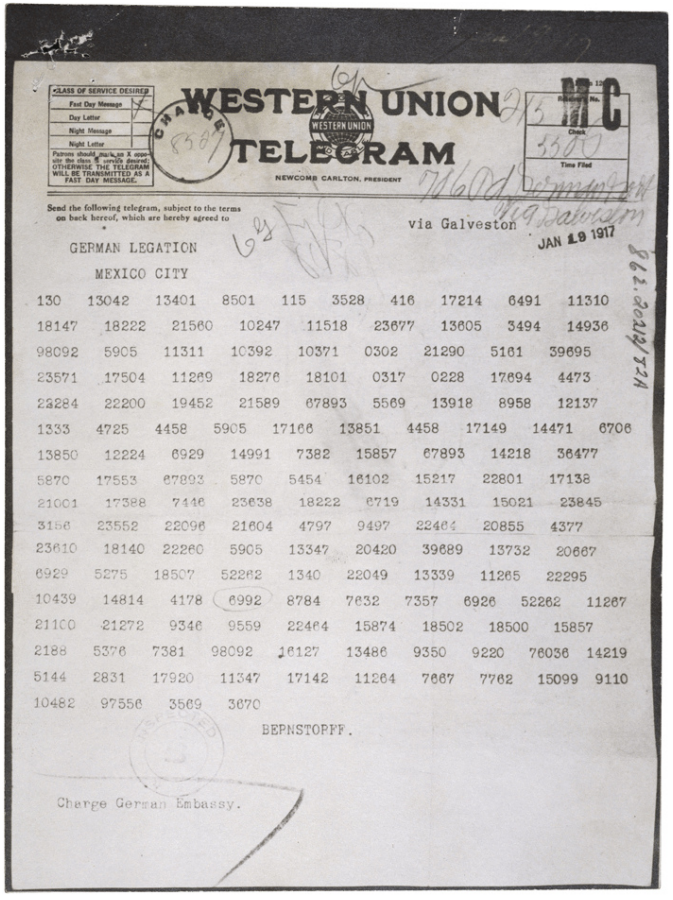
1883. Auguste Kerckhoffs: La cryptographie militaire

Kerckhoffs stellt sechs "Desiderata der militärischen Kryptographie" auf.

Das Kerckhoffs'sche Prinzip kurz und knapp:

> Das Geheimnis darf nur im Schlüssel liegen, und dieser muss noch während der Kommunikation veränderbar sein.

Das Ende



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

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

via Galveston

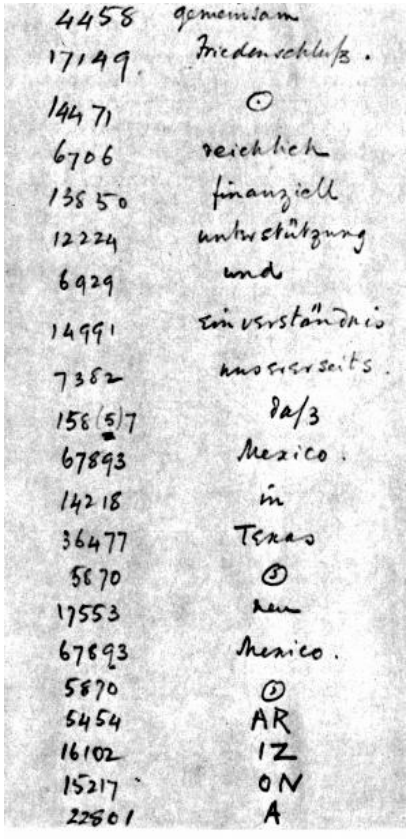
JAN 19 1917

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
5870 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

BEPNSTORFF.

Charge German Embassy.



4458 gemeinsam
17149 Friedensschluß.
14471 ⊙
6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 einverständnis
7382 unserseits.
15857 Da/3
67893 Mexico
14218 in
36477 Texas
5870 ⊙
17553 New
67893 Mexico.
5870 ⊙
5454 AR
16102 IZ
15217 ON
22801 A

Die Zimmermann-Depesche (Zimmermann telegram) (19.1.1917)

Quelle. General Records of the Department of State

Die Periode der elektrisch-mechanischen Chiffriermaschinen

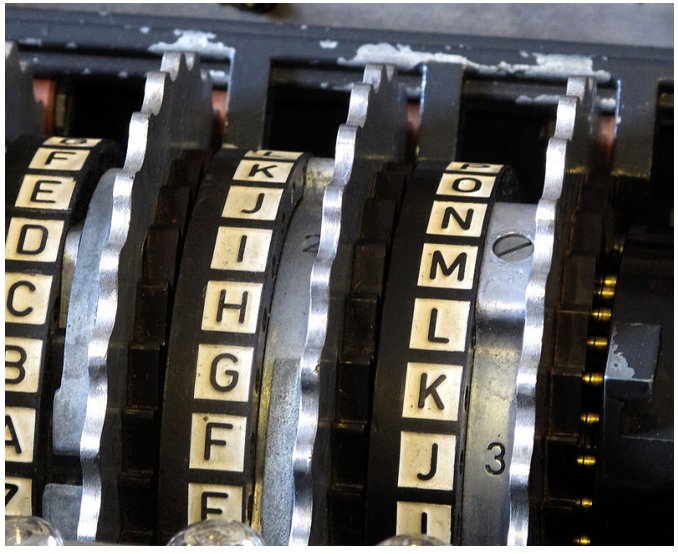
Neue Entwicklungen

1917. one time pad von Gilbert Vernam (AT & T), Joseph Mauborgne (US Army Signals Corps)

Auch ab ca. 1917. Rotormaschinen von

- Theo van Hengel, R. Sprengler (1915, NL)
- Edward Hebern (1917, US)
- Arthur Scherbius (1918, D) (Enigma)
- Arvid Damm (1918, S) ($\rightarrow$ Crypto AG, CH)
- Hugo Koch (1918-19, NL)

Die Enigma-Maschinen

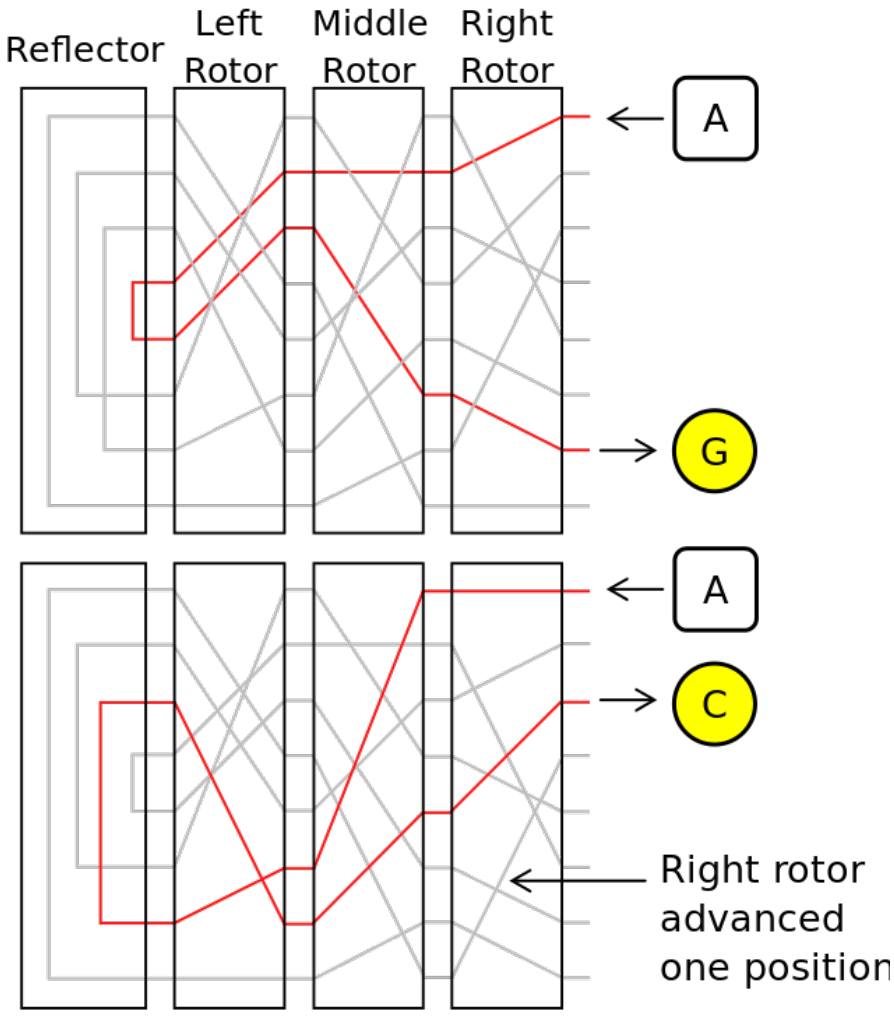


Quellen.

Museo della Scienza e della Tecnologia “Leonardo da Vinci” / Wikipedia

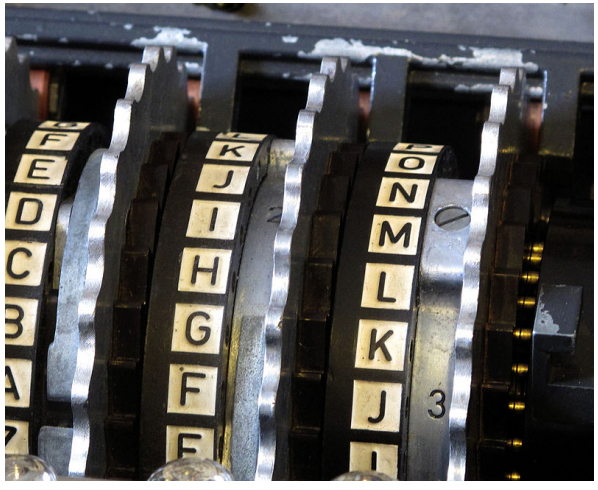
Wikipedia

Die Enigma-Maschinen



Quelle. Wikipedia, Benutzer MesserWoland, Jeanot, Math Crypto

Die Enigma-Maschinen



Quellen.

Museo della Scienza e della Tecnologia “Leonardo da Vinci” / Wikipedia

Wikipedia

Die Enigma-Maschinen

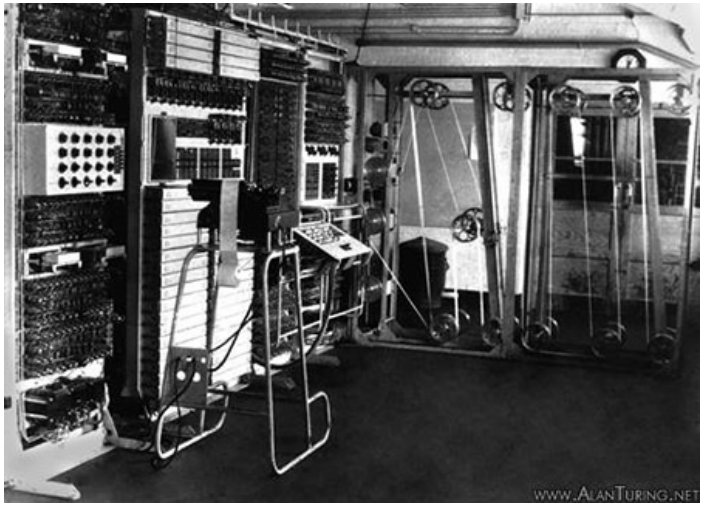
Quellen.

Museo della Scienza e della Tecnologia “Leonardo da Vinci” / Wikipedia

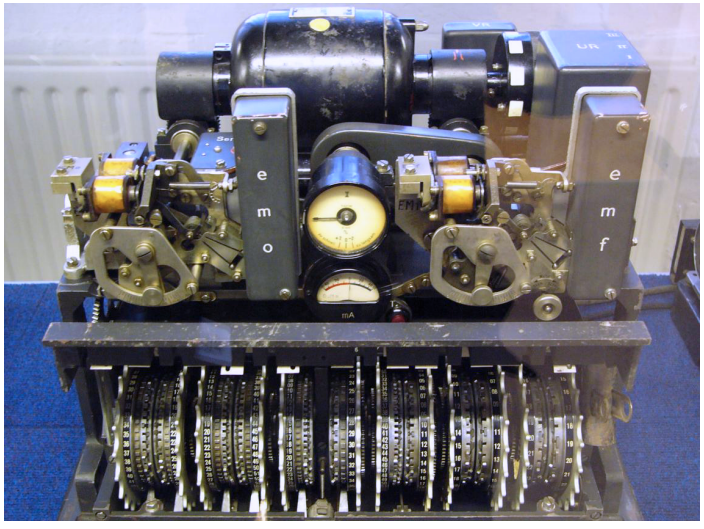
Ben Slivka / Wikipedia

Aliierte Kryptoanalyse im II. Weltkrieg

1943



Colossus



Lorenz-Maschine

Quellen.

British National Archive

Wikipedia

Das elektronische Zeitalter

Wissenschaftliche Grundlagen

ca. 1948. Claude Shannon: Communication Theory of Secrecy Systems

- Begriff der “perfekten Sicherheit”
- Diese erfordert, dass der Schlüssel (mindestens) so lang ist wie der Klartext.
- Ideen der Konfusion und Diffusion

Computer

Seit “Colossus”. Computer werden zur Kryptoanalyse eingesetzt (?).

In den 1960gern. Elektronische Datenverarbeitung (EDV) kommt auf.

Die Grundeinheit (“Atom”) der Informatik ist nun das Bit.

DES

1973-1977. Der Digital Encryption Standard (DES) wird ausgeschrieben und verarbschiedet.

Entwicklung in Kooperation mit IBM, teilweise geheim

Eine Blockchiffre

basierend auf Shannons Konfusions-Diffisions-Paradigma

Exkurs: DES

Substitutions-Permutations-Netzwerke

eine Anwendung von Shannons Konfusions-Diffusions-Paradigma

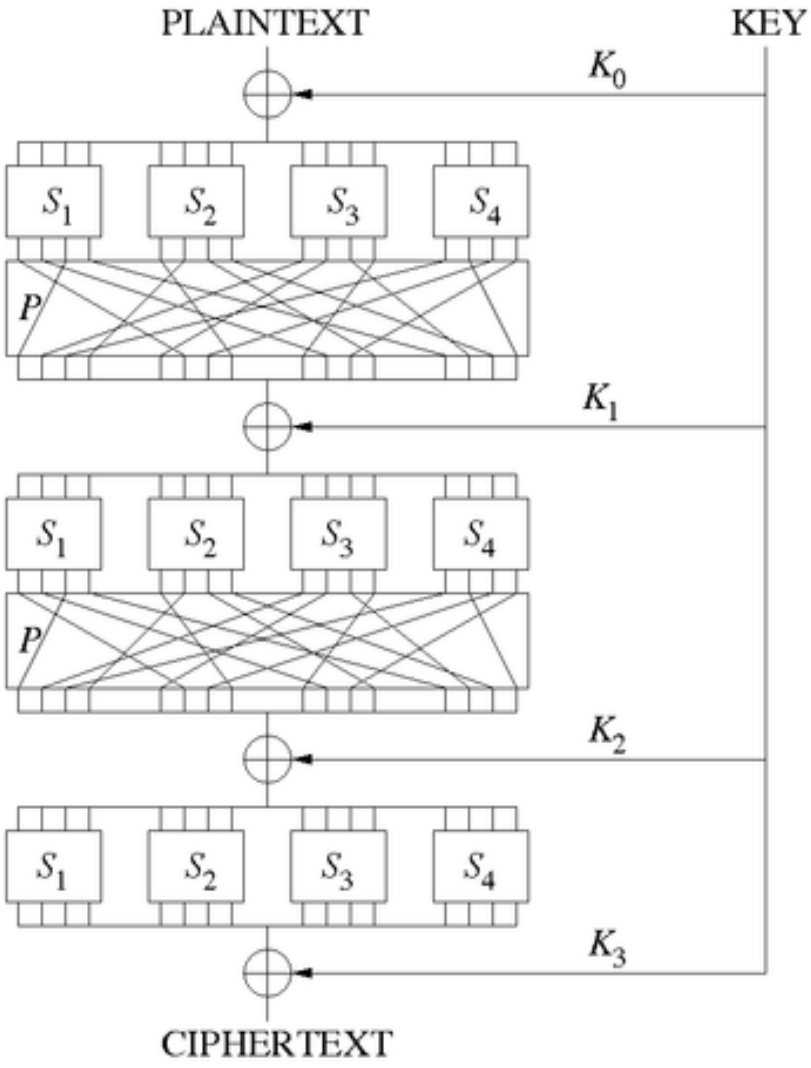
Substitution = kurze Bitstrings werden durch andere Bitstrings ersetzt
$\rightarrow$ Konfusion

mittels einer S-Box

Permutation = Transposition (in "Krypto-Sprache") = Reihenfolge der Bits wird vertauscht
$\rightarrow$ Diffusion

mittels einer P-Box

Substitutions-Permutations-Netzwerke



S_i. S-Box

P. P-Box

K_i. Rundenschlüssel

Quelle. Wikipedia, Benutzer GaborPete

Feistel-Netzwerke

Operation in Runden

In Runde i:

Es sei eine "Nachricht" M_i und ein Rundenschlüssel K_i gegeben.

Die Nachricht wird aufgeteilt: $M_i = L_i \parallel R_i$.

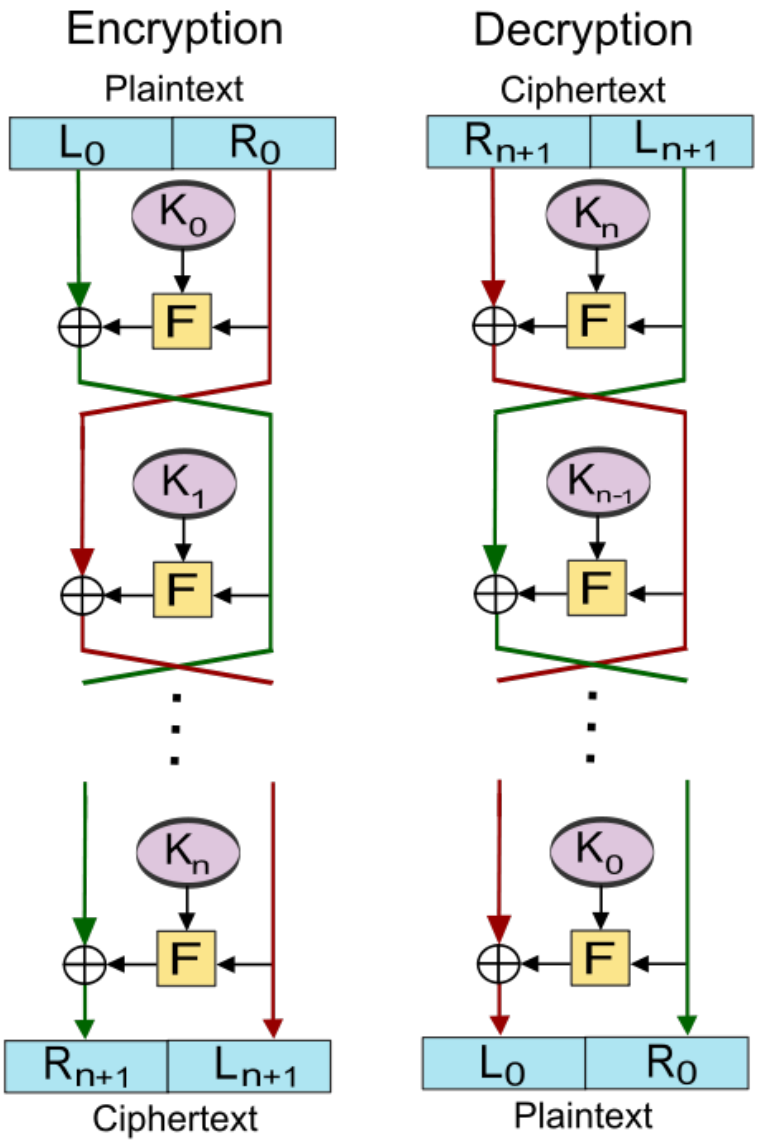
Es wird gesetzt:

$$L_{i+1} := R_i \quad , \quad R_{i+1} := L_i \oplus F_{K_i}(R_i)$$

für eine feste Funktion F (Feistel-Funktion).

Damit ist $M_{i+1} = L_{i+1} \parallel R_{i+1}$.

Feistel-Netzwerke



F muss nicht invertierbar sein!

Quelle. Wikipedia, Benutzer Amirki

Feistel-Netzwerke

Verschlüsselung

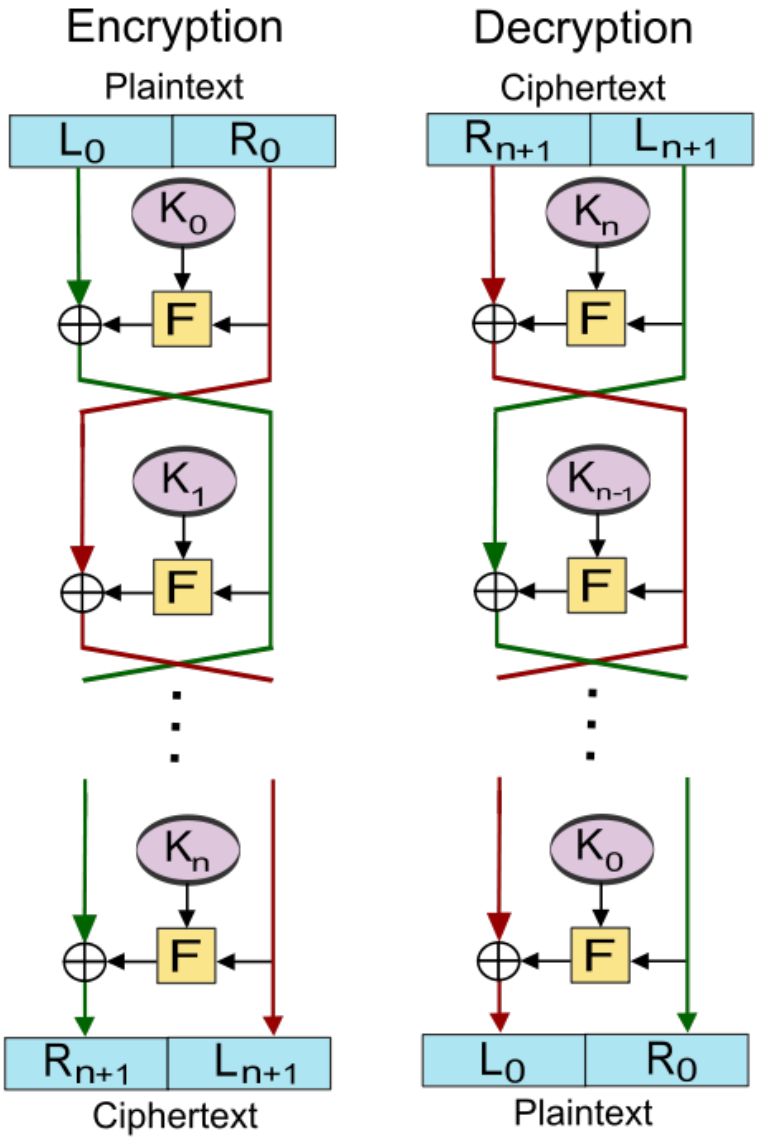
$$L_{i+1} = R_i \quad , \quad R_{i+1} = L_i \oplus F_{K_i}(R_i)$$

Entschlüsselung

$$R_i = L_{i+1} \quad , \quad L_i = R_{i+1} \oplus F_{K_i}(R_i)$$

Nicht vergessen! Man braucht auch noch den Schlüsselplan (key schedule).

Feistel-Netzwerke



Graphik: Wikipedia, Benutzer Amirki

DES

Feistel-Chiffre bestehend aus 16 Runden.

Jede Runde (im Wesentlichen):

- Einmischen des Rundenschlüssels mittels XOR
- Substition mit S-Boxen: 6 Bit $\rightarrow$ 4 Bit
- Transposition der Blöcke

Schlüssellänge (nur) 56 Bit.

Wieso sind die S-Boxen so wie sie sind?

Kryptoanalyse

1977. Diffie & Hellman. Kann mit 20 mio $ gebrochen werden.

1997. Wettbewerb von RSA, erfolgreich

1998. Maschine für 250.000 $

2006. COPACOBANA für 10.000 €

2008. COPACOBANA in einem Tag

AES

1997 - 2000. Der Advanced Encryption Standard (AES) wird ausgeschrieben und verarbschiedet.

Es gewinnt das Verfahren Rijndael.

Permutations-Substitutions-Netzwerk mit "mathematischen" S- und P-Boxen.

S-Box. "Im Wesentlichen" gegeben durch:

$$\mathbf{F}_{2^8} \longrightarrow \mathbf{F}_{2^8}, \quad a \mapsto a^{-1} \text{ für } a \neq 0\ ,\ 0 \mapsto 0$$

Passwörter

ab ca. 1965

Problem mit Aufkommen der Großrechner:

Es sollen Passwörter geschützt werden (auch vor dem Administrator!).

Idee von Roder Needham 1967. Man benutzt einen "Einweg-Cipher" (Maurice Wilkies) :

Gesucht ist eine Funktion f, die schnell berechnet werden kann, für die es aber de facto unmöglich ist, zu einem $C = f(P)$ ein P' mit $f(P') = C$ zu finden.

("Einwegfunktion")

Heutzutage: Kryptographische Hash-Funktionen

Neue Grundlagen

1960ger. Theoretische Informatik entsteht als eigenständiges Gebiet, insbesondere Komplexitätstheorie

- qualitative Analyse von Algorithmen
- Einführung der Komplexitätsklassen (P,NP,BPP, ...)

Neue Richtungen

1976. Whitfield Diffie & Martin Hellman. New Directions in Cryptography,
IEEE Transactions on Information Theory

Neue Richtungen

Whitfield Diffie & Martin Hellman. New Directions in Cryptography:

- Ein Protokoll zum Schlüsselaustausch
- Qualitative, komplexitätstheoretische Definition von "Einwegfunktion"
- Propagieren eines komplexitätstheoretischen Zugangs

Exkurs: Das Diffie-Hellman-Protokoll

Modulorechnen

Es sei p eine Primzahl.

Wir haben die Menge der Restklassen

$$\mathbf{Z}/p\mathbf{Z} \ .$$

Beispiel.

$$\mathbf{Z}/11\mathbf{Z} = \{[0]_{11}, [1]_{11}, \ldots, [10]_{11}\}$$

$$[11]_{11} = [0]_{11} \ , [24]_{11} = [13]_{11} = [2]_{11} = [-9]_{11}$$

$$[5]_{11} + [6]_{11} = [11]_{11} = [0]_{11}$$

$$[3]_{11} \cdot [4]_{11} = [12]_{11} = [1]_{11}$$

$\mathbf{Z}/p\mathbf{Z}$ ist ein Körper mit Null-Element $[0]_p$ und Einselement $[1]_p$.
Bezeichnung: $\mathbf{F}_p$. Die multiplikative Gruppe ist

$$\mathbf{F}_p^* = \mathbf{F}_p \backslash \{[0]_p\} = \mathbf{F}_p \backslash \{0\} \ .$$

Die Ordnung

Für $a \in \mathbf{F}_p^*$ betrachten wir

$$\langle a \rangle := \{a^0 = 1\,,\, a^1 = a\,,\, a^2\,,\, \ldots\,,\, a^i\,,\, \ldots\}\,.$$

Die Anzahl $\#\langle a \rangle = \{a^i \mid i \in \mathbf{N}_0\}$ heißt die Ordnung von a, $\mathrm{ord}(a)$.

Es ist $\langle a \rangle = \{a^0 = 1\,,\, a^1 = a\,,\, a^2\,,\, \ldots\,,\, a^{\mathrm{ord}(a)-1}\}$,

$$a^{\mathrm{ord}(a)} = a^0 = 1\,.$$

Beispiel. Es ist

$$[4]_{11}^2 = [5]_{11}\,,\; [4]_{11}^3 = [9]_{11}\,,\; [4]_{11}^4 = [3]_{11}\,,\; [4]_{11}^5 = [1]_{11} = 1$$

und somit $\mathrm{ord}([4]_{11}) = 5$.

Das Diffie-Hellman-Protokoll

Alice und Bob einigen sich (in der Öffentlichkeit) auf eine große Primzahl p und ein Element $a \in \mathbf{F}_p^*$.

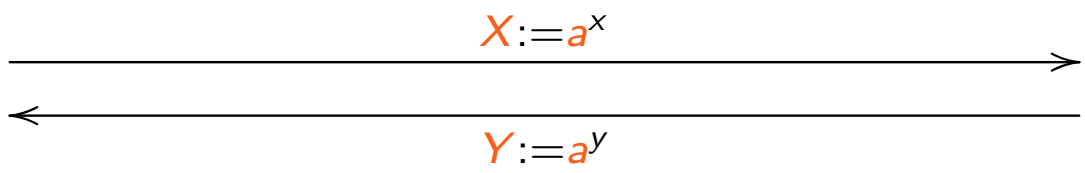
Alice		**Bob**
Wählt $x < \mathrm{ord}(a)$.		Wählt $y < \mathrm{ord}(a)$.
	$X := a^x$ →	
	← $Y := a^y$	

$$\boxed{Y^x = a^{xy} = X^y}$$

Das Diffie-Hellman-Protokoll

Alice und Bob einigen sich (in der Öffentlichkeit) auf eine große Primzahl p und ein Element $a \in \mathbf{F}_p^*$.

Alice	**Bob**
Wählt $x < \mathrm{ord}(a)$.	Wählt $y < \mathrm{ord}(a)$.



$$\boxed{Y^x = a^{xy} = X^y}$$

Zur Sicherheit

Zur Sicherheit des Protokolls:

- Für die Sicherheit des Protokolls ist das Diffie-Hellman Problems relevant:

  Gegeben $p; a, X = a^x, Y = a^y$, berechne a^{xy}.
- Hierfür ist insbesondere die Schwierigkeit des klassischen diskreten Logarithmusproblems relevant:
  Gegeben $p; a, X = a^x$, berechne x.
- Wir haben eine Reduktion vom DHP auf das DLP (DHP $\leq$ DLP)

Das Diffie-Hellman-Protokoll

Alice und Bob einigen sich (in der Öffentlichkeit) auf eine große Primzahl p und ein Element $a \in \mathbf{F}_p^*$.

Alice		**Bob**
Wählt $x < \mathrm{ord}(a)$.		Wählt $y < \mathrm{ord}(a)$.
	$X := a^x$ →	
	← $Y := a^y$	

$$\boxed{Y^x = a^{xy} = X^y}$$

Zur Sicherheit II

Nach einigem Nachdenken:

- Das Protokoll ist für Parameter p, a genau dann sicher gegenüber Lauschern, wenn das entsprechende Diffie-Hellman Problem nicht gelöst werden kann:

  Gegeben $X = a^x$, $Y = a^y$, berechne a^{xy}.
- Hierfür ist insbesondere die Schwierigkeit des klassischen DLP zu p, a relevant:
  Gegeben $X = a^x$, berechne x.
- Das Protokoll ist vollkommen unsicher gegenüber aktiven Angreifern.
- Authentisierung fehlt!
- Für ein Protokoll mit Authentisierung will man zweigen: Jeder effiziente Angriff aus einer großen Angriffsklasse führt zu einem effizienten Algorithmus für das DHP (oder besser: für das DLP) (reduktives Sicherheitsresultat).

Beginn einer Diskussion

Angeregt durch das Diffie-Hellman-Verfahren:

- Was sollte eigentlich “das Verfahren ist sicher” bedeuten?
- Kann man allgemeine Angriffsmethoden definieren?
- Kann man die Sicherheit von Protokollen auf die Sicherheit unterliegender Algorithmischer Probleme zurückführen?

Verwissenschaftlichung

Ab 1981/82. Crypto, Eurocrypt

Verwissenschaftlichung

Entwicklung einer theoretischen Kryptographie /
Interativen Komplexitätstheorie (C.D.)

- Absolute Aussagen sind unmöglich:
  Wenn $P = NP$ “bricht alles zusammen”.
- Aussagen der Form

  Wenn das algorithmische Problem X schwer ist (im Sinne von ...), ist das Verfahren sicher im Sinne von ...

Verwissenschaftlichung

Verbindung zur Zahlentheorie

und ab ca. 1990 zur algebraischen Geometrie (mittels elliptischen Kurven)

und damit zur “reinen Mathematik”

vgl. Godfrey Harold Hardy in A Mathematicians Appology (1940):

> *’real’ mathematics is harmless and innocent*
>
> *No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity.*

Alles wird verbunden

Ab ca. 1992. Miniaturisierung macht Smartcards möglich
$\rightarrow$ Digitale Signatur, Authentisierung und weitere Anwendungen

Ab ca. 1994. “Internet” (als Massenphänomen)

Theorie und Parxis

2000, 2004. Konsolidierung der Theorie durch die *Foundations of Cryptography* von Oded Goldreich

Ab ca. 1993. Versuche, die Lücke zwischen Theorie und Praxis zu schließen

Lücke bleibt bestehen ...

Neueste (gute) Versuche:

- Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography (2015)
- Dan Boneh, Victor Shoup. A Graduate Course in Cryptography (2009 - ...?)

Zur dieser Vorlesung “Kryptographie”

Inhalt der Vorlesung “Kryptographie”

- Einführung in den komplexitätstheoretischen Zugang zur Kryptographie
- Klärung einiger grundlegender Begriffe und des allgemeinen Vorgehens

Im Konkreten (geplant):

§0 Einführende Worte (✓)

§1 Geschichtlicher Überblick (✓)

§2 Zufall

§3 Grenzen der perfekten Sicherheit

§4 Der komplexitätstheoretische Ansatz

§5 Pseudozufallsgeneratoren und Stromchiffren

§6 Pseudozufallsfunktionen und Blockchiffren

Warum?

Komplexitätstheorie ist abstrakt und teilweise “trocken”.

Warum so ein “theoretischer Überbau”?

- “Sicher” ist ein sehr schwammiger Begriff.
  “Das Verfahren ist sicher” ist ohne Erläuterung zu “sicher” inhaltsleer und / oder absurd und / oder eine “Glaubenssache” / eine autoritäre Aussage.
- Man macht wirklich Fehler, wenn man nicht-rigorose ad-hoc-Überlegungen macht.
- Auch “sichere” “Bausteine” (“kryptographische Primitive”) führen nicht direkt zu sicheren Verfahren (und das ist nicht immer leicht zu sehen).

Warum?

Der theoretische "Überbau" hilft dabei, unklare und / oder klar manipulative Aussagen zu erkennen, wie z.B.:

Wikipedia: Diffie-Hellman-Schlüsselaustausch
Der DHM-Schlüsselaustausch zählt zu den Krypto-Systemen auf Basis des diskreten Logarithmus (kurz: DL-Verfahren). Diese basieren darauf, dass die diskrete Exponentialfunktion in gewissen zyklischen Gruppen eine Einwegfunktion ist.

Wikipedia: Multivariate cryptography
Multivariate cryptography is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over a finite field ... Solving systems of multivariate polynomial equations is proven to be NP-hard or NP-complete. That's why those schemes are often considered to be good candidates for post-quantum cryptography.

Das ist nicht alles ...

Auch diesen "Überbau" ist aber nicht alles Wichtige gesagt,

es gibt noch andere Aspekte:

- Algebraische Grundlagen für die Kryptographie mit öffentlichen Schlüsseln
- Teilweise: Parameterwahl
- Teiweise: "Bewährte Ingenieurprinzipien"
- Angriffe (weit) außerhalb der betrachteten Angriffsmodelle:
  - Fehler in Soft- und Hardware (echte Fehler und auch "Unterjubeln")
  - Abstrahlung in einem weiten Sinne
  - Benutzerverhalten

Immer beachten! Menschen machen auch Fehler.