Kryptographie

Jan Fässler

3. Semester (HS 2012)

If you use this documentation for a exam, you should offer a beer to the authors!

Inhaltsverzeichnis

1 Klassische Kryptologie

1.1 Repetitionen

Alphabet endliche Mengen von Zeichen

Beispiel
$\Lambda := \{A, B, C, ..., Z\}$, $|\Lambda| = 26$
$\Sigma := \{0, 1\}$, $|\Sigma| = 2$

Sprache über $\Lambda : L \subset \Lambda^*$

1.2 Klassifizierungen

Substitution Cipher	**Transposition Cipher**
Einheiten werden **ersetzt**.	Einheiten werden **vertauscht**. 3 1 5 6 2 4 K O M M E H E U T E A B E N D Z U M Z O O A B C ABC = padding $\rightarrow$ OUNOEAUBK...

mono-alphabetische Cipher	**poly-alphabetische Cipher**
$E : A \rightarrow B$ $x \rightarrow E(x)$ Buchstaben	$E : A \rightarrow P(B)$ $x \rightarrow E(x)$ Gruppen von Buchstaben

1.3 Homophone Verschlüsselung

Gegeben $\sum := \{0, 1\}$, $B := \{a, b, c\}$

Informationen über die Sprache des Klartextes:
Häufigkeit von $0 = \frac{1}{3}$
Häufigkeit von $1 = \frac{2}{3}$

$$E : \sum \rightarrow P_{(B)} \tag{1}$$
$$0 \rightarrow \{b\} \tag{2}$$
$$1 \rightarrow \{a, c\} \tag{3}$$

Beispiel:
10110110011
abccbacbbaa

1.4 Kaski - Text

Klartext TO BE OR NOT TO BE

Schlüssel NOW

T	O	B	E	O	R	N	O	T	T	O	B	E
N	O	W	N	O	W	N	O	W	N	O	W	N
G	C	X	R	C	N	A	C	P	G	C	X	R
–	–	–	–						–	–	–	–

1.5 Polyfair-Cipher

tbd.

1.6 Koinzidenzindex

1) Gegeben

Alphabet $\Lambda := \{A, B, C, ..., Z\}$
Sprache: Englisch

$\rightarrow$ Buchstabenhäufigkeit: $\begin{matrix} p_A & p_B & \cdots & p_Z \\ " & " & & " \\ p_1 & p_2 & \cdots & p_3 \end{matrix}$

mit $0 \leq p_i \leq 1$ und $\sum_{i=1}^{26} p_i = 1$

IC: Grösse, die von der Sprache abhängt, aber invariant ist gegenüber Cäsar-Verschiebungen.

Frage: Was bedeutet: $IC_L := \sum_{i=1}^{26} p_i^2$?

Bemerkung:

Jede Sprache hat ihren eigenen Konzidenzindex
$IC_{German} = 0.0766$
$IC_{Arabic} = 0.0759$
$IC_{flat} = 0.0385$ (Alle Buchstaben haben die gleiche häufigkeit: $p_1 = p_2 = ... = p_{26} = \frac{1}{26}$)
Je unregelmässiger die buchstabenhäufigkeit, umso grösser der Index.

2) Gegegen:

Sei F eine buchstabenfolge der Länge n
Bsp: F= "AXCAABCXA"

Frage: Wie gross ist die Wahrscheinlichkeit zwei gleiche Buchstaben aus F herauszugreifen?

Definition $IC_F = \frac{\sum_{i=1}^{26} \binom{n_i}{2}}{\binom{n}{2}}$

Bsp:

Alphabet $\Sigma := \{0, 1\}$
F = 00110111101

$$\left.\begin{array}{r} n_0 = 4 \\ \underline{n_1 = 7} \\ n = 11 \end{array}\right\} IC_F = \frac{4*3+7*6}{11*10} = 0.49$$

Annahme $IC_F \xrightarrow[F\to\infty]{} IC_L$ ($i * A$ ist das falsch)

Bemerkung

Permutation der buchstaben
F $\rightarrow$ Perm(F)
F = "AXCA ...."$\rightarrow$ Perm(F) = "CBYC..."
$IC_F = IC_{Perm(F)}$

1.7 Vigenères Chipres

1.7.1 Berechnung der Schlüssellänge

Gegeben

C Vigenère-Chiffrat der Länge n
Die Schlüssellänge sei p (unbekannt)

p = Spalten

$$\left.\begin{array}{ccccc} C_1 & C_2 & C_3 & ... & C_p \\ C_{p1} & C_{p2} & C_2 & ... & C_{2p} \\ .. & .. & .. & .. & .. \\ C_{n-2} & C_{n-1} & C_n & - & - \end{array}\right\} \text{n/p}$$

$\alpha :=$ Anzahl Buchstabenpaare aus gleicher Spalte

$\alpha = \frac{n(\frac{n}{p}-1)}{2} = \frac{n(n-p)}{2p}$

$\beta :=$ Anzahl Buchstabenpaare aus verschiedenen Spalte

$\beta = \frac{n(n-\frac{n}{p})}{2} = \frac{n^2(p-1)}{2p}$

$\gamma :=$ Anzahl gleicher Buchstabenpaare aus C

$IC_c = \frac{\gamma}{\binom{n}{2}}$

$\gamma = \alpha * IC_L + \beta * IC_{flat}$

Beispiel

$p = \frac{n(IC_L - IC_{flat})}{IC_C(n-1)+IC_L-n*IC_{flat}}$

1.7.2 Kryptoanalysis

1) Schlüssellänge p

p=1,2,3,...

- Einleitung des Cipher-Tests in p Abschnitte
- Berechnung des IC des Abschnitts
- Wähle p mit $IC \sim IC_2$ (oder hoch)

2) Sei s,t zwei Strings über dem Alphabet A.

$s = s_1, s_2, s_3, ...s_k$

$t = t_1, t_2, t_3, ..., t_l$

Wieder zählen wir $n_1(s) :=$ A in s, $n_3(t) =$ C in t

Def. $MIC(s,t) := \frac{\sum_{i=1} 26 n_i(s)*n_i(t)}{k*l}$

Bsp.

s="AABCCA"

t=ÄBCABCABC"

$n_1(s) = 3$, $n_1(t) = 3$

$n_2(s) = 1$, $n_2(t) = 3$

$n_3(s) = 2$, $n_3(t) = 3$

$\rightarrow MIC(s,t) = \frac{1}{6*9}[3*3+1*3+2*3]$

Idee: s,t zwei cipher-Text mit Cäsar Cerschlüsselung

Wenn beide mit dem gleichen Schlüssel verschlüsselt werden

$\rightarrow MIC(s,t) \rightsquigarrow IC_L$

Sonst: $MIC(s,t) \rightsquigarrow IC_{flat}$

3.) Anwendung auf Cipher Text

Schlüssellänge p sei 5

$c_1, c_2, ..., c_5$ Abschnitte des Cipher Text

$MIC(c_i, c_j + k)$

Tabelle:

$k_{ij} \backslash k$	0	1	2	3	...	
(1,2)						
(1,3)						
(1,4)						
(1,5)						
(2,3)			x			$\rightarrow MIC(c_2, c_3 + k)$
(2,4)						
(2,5)						
(3,4)						
(3,5)						
(4,5)						

Bsp

c_1:	AXBM...
c_3:	ABXHE...
$c_3 + 2$:	CDZJG

4.) Wir suchen Einträge in der Tabelle, die hoch sind (> 0.06)
zb: $MIC(c_2, c_3{+}22 > 0.06 \iff c_2 \sim c_3 + 22 \Rightarrow \beta_2 - \beta_3 = k$

Notation s~t $\iff$ s und t sind mit dem gleichen Shift aus zwei Klartexten entstanden.

Bsp. $klar_1 \sim klar_2$

$$\begin{array}{l|l} klar_1 \xrightarrow{\beta_1} c_1 & c_1 = klar_1 + \beta_1 \\ klar_2 \xrightarrow{\beta_2} c_2 & c_2 = klar_2 + \beta_2 \end{array}$$

Wir suchen die grossen Werte von $MIC(c_i, c_j + k)$
$MIC(c_i, c_j + k)$ gross $\iff c_i \sim c_j + k$

$c_i = klar_i + \beta_i \sim klar_i + \beta_j + k = k = \beta_i + \beta_j$

$k_{1,2} = \beta_2 - \beta_1$
$k_{1,3} = \beta_3 - \beta_1$
$k_{5,2} = \beta_2 - \beta_5$
$\rightarrow$ Auflösen nach β_1 ($k_{x,y}$ sind bekannt $\rightarrow$ Tabelle)

Schlüsselwort: $\beta_1, \beta_2, ..., \beta_p = \beta_1, \beta_1 + k_{1,2}, ...$
Ausprobieren: $\beta_1 = 0, 1, ..., 25$

1.8 One-Time-Pad

$\sum = \{0, 1\}$

Klartext:	$p_1\ p_2\ p_3\ p_4\ p_5$ ...	= 00101 ...
Schlüssel:	$k_1\ k_2\ k_3\ k_4\ k_5$ ...	= 10110 ...
Cipher-T:	$c_1\ c_2\ c_3\ c_4\ c_5$ ...	= 10011 ...
	$\rightarrow (p_1 \oplus k_1)$	

1.9 Kryptosysteme

Kryptosystem: (P, C, K, e, d)

P Menge der Klartexte

C Menge der Geheimtexte

K Menge der Schlüssel

$e : K \times P \to C$
$d : K \times C \to P$

$\forall k \varepsilon K \; \forall p \varepsilon P : d(k, e(k,p)) = p$
$\to \forall k \varepsilon K : e(k, -)$ ist injektiv
$\to \forall k \varepsilon K : d(k, -)$ ist surjektiv

1.10 Kryptoanalysis

1.10.1 Ciphertext-only attack

Gegeben $c_i = e_k(p_i)$, i=1, ..., n

Gesucht p_i, i= 1, ...,n oder k

1.10.2 known-plaintext attack

Gegeben (p_i, $c_i = e_k(p_i)$), i=1, ..., n

Gesucht k

1.10.3 chosen-plaintext attack

Gegeben (p_i, $c_i = e_k(p_i)$), i=1, ..., n
p_i nach Wahl des Kryptoanalytikers

Gesucht k

Verwendung DIE Attacke gegen jedes Public-Key System

1.10.4 chosen-ciphertext attack

Gegeben (p_i, $p_i = d_k(c_i)$), i=1, ..., n
c_i nach Wahl des Kryptoanalytikers

Gesucht k

2 Block-Cipher

Alphabet

$\sum=\{0,1\}$
$\sum^n := \sum \times \sum \times ... \times \sum$

Definition

Ein Block - Cipher ist eine **injektive** Abbildung
$C : K \rightarrow Perm(\sum^n)$
wobei K der Schlüsselraum ist.

Bsp.

$n = 3$
$\sum^3 = \sum \times \sum \times \sum$

Frage:

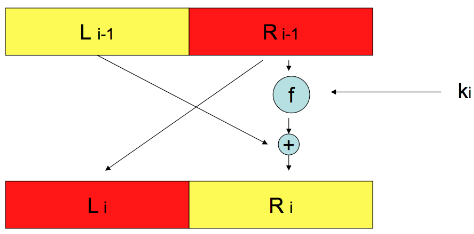
Wie gross ist der Schlüsselraum K maximal?
$|K| \leq (2^n)!$

2.1 Data Encription Standard (DES)

Lucifer : Schlüssellänge 128

$\downarrow$

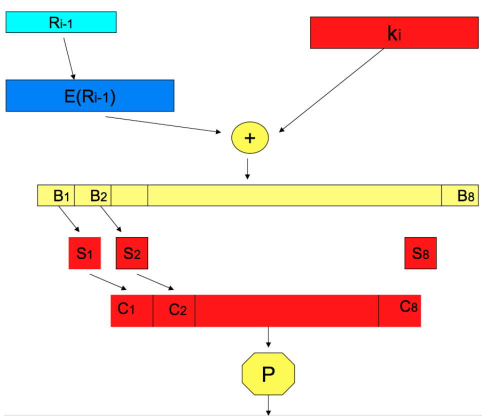
DES : Schlüssellänge 56
Blocklänge 64



$$L_1 := R_0 \tag{4}$$
$$R_1 := f(R_0, k_1) \oplus L_0 \tag{5}$$

$$L_0 := f(L_1, k_1) \oplus R_1 \tag{6}$$
$$R_0 := L_1 \tag{7}$$

Die f-Funktion:



2.2 Modi von Blocksipher

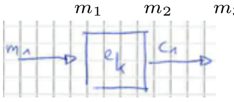
Sei $\sum := \{0, 1\}$
P = C = $\sum^4$
k = Permutationen von $\sum^4$
k = π = $(\frac{1234}{2134})$

Vor und Entschlüsselung

Sei m=01001 $\in$ P (Klartext)
$e_k(m) = e_k(10101) = 1010 = C$

2.2.1 ECB-Modul (Electornic Code Block)

$m = \underbrace{1100}_{m_1} | \underbrace{0110}_{m_2} | \underbrace{1100}_{m_3} | 101*$



Bem. 1) $m_1 = m_3 \Rightarrow c_1 = c_3$

Bem. 2) Vertauschen der Ciphertext-Blöcke wird nicht notwendigerweise erkannt.

2.2.2 CBC-Modi

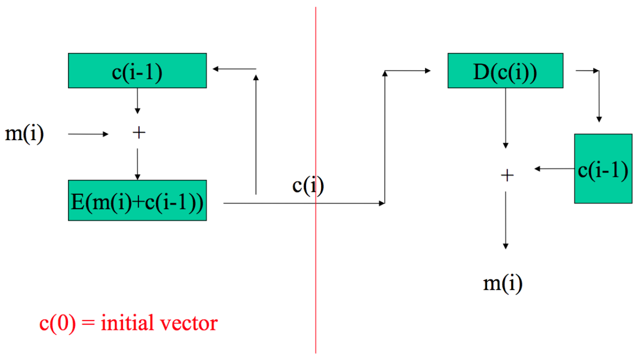
$m = m_1 | m_2 | ...$

IV = Initialvektor (i.a. bekannt)
$C_0 := IV$
$C_1 := e_k(C_0 \oplus m_1)$
$C_2 := e_k(C_1 \oplus m_2)$

$m = \underbrace{1100}_{m_1} | \underbrace{0110}_{m_2} | \underbrace{1100}_{m_3} | 101$
$IV = C_0 = 1110$

$c_1 = e_k(c_0 \oplus m_1) = e_k(0010) = 0001$
$c_2 = e_k(c_1 \oplus m_2) = e_k(0111) = 1011$
$c_3 = e_k(c_2 \oplus m_3) = e_k(0111) = 1011$

Entschlüsselung: $c_1 \oplus d_k(c_2) = c_1 \oplus d_k(e_k(c_1 \oplus m_2)) = c_1 \oplus m_2 \oplus c_1 = m_2$



Bem 1) $m_1 = m_3 \not\Rightarrow c_1 = c3$

Bem 2) Vertauschen kann bemerkt werden

Bem 3) Übertragungsfehler machen sich bemerkbar.

2.2.3 CFB-Modi (cipher feedback)

$m = \underbrace{m_1}_{r}|m_2|m_3|...$

n: Cipher Block Länge (DES:64)

und $0 < r \leqslant n$

$m = \underbrace{110}_{m_1}\underbrace{001}_{m_2}\underbrace{101}_{m_3}\underbrace{100}_{m_4}\underbrace{101}_{m_5}$

IV = 1110

r=3 / n=4