Kryptographie Vorlesungsnotizen

Jan Fässler & Fabio Oesch

4. Semester (FS 2013)

Inhaltsverzeichnis

1 Klassische Kryptographie

1.0 Repetition

Alphabet endliche Mengen von Zeichen

Beispiel

$\mathcal{A} := \{A, B, C, ..., Z\}$, $|\mathcal{A}| = 26$
$\Sigma := \{0, 1\}$, $|\Sigma| = 2$
$\mathcal{A}^* := \{\text{endliche Wörter über } \mathcal{A}\}$

Sprachen über $\mathcal{A}$: $L \subset \mathcal{A}^*$

1.1 Klassische Verschlüsselungsverfahren

Substitution Cipher	**Transposition Cipher**
Einheiten werden **ersetzt**.	Einheiten werden **vertauscht**. $\begin{array}{cccccc} 3 & 1 & 5 & 6 & 2 & 4 \\ \hline K & O & M & M & E & H \\ E & U & T & E & A & B \\ E & N & D & Z & U & M \\ Z & O & O & A & B & C \end{array}$ $\Rightarrow \underbrace{\text{OUNO}}_{1}\underbrace{\text{EAUB}}_{2}\ldots$ **Bem.** Einheiten werden vertauscht (ABC ist Padding)

monoalphabetisch $E : \mathcal{A} \to B$, $x \mapsto E(x)$	**polyalphabetisch** $E : \mathcal{A} \to P(B)$, $x \mapsto E(x)$
monographisch Buchstaben	**polygraphisch** Gruppen von Buchstaben

1.2 Spezielles Bsp für Substitution Homophone Verschlüsselung

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

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

$$\begin{aligned} E :& \Sigma \to P(B) \\ & 0 \mapsto \{b\} \\ & 1 \mapsto \{a, c\} \end{aligned}$$

Bsp: 10110110011
abccbacbbaa

1.3 Kasiski-Text (monographisch & polyalphabetisch)

Klartext TO BE OR NOT TO BE

Schlüssel NOW

p = |NOW|

TOB	EOR	NOT	TOB	E
NOW	NOW	NOW	NOW	N
GCX	RCN	ACP	GCX	R

GCX kommt 2x for so können wir eine Annahme zur Periode p machen. Die Periode ist dann $c \cdot p$. Dies kann aber auch zufällig passieren.

1.4 Playfair-Cipher

HARYP
OTEBC
DFG$\frac{I}{J}$K
LMNQS
UVWXZ

Schlüssel: Harry Potter, HAR~~R~~Y POT~~T~~E~~R~~

	Klartext	HA	LL	O	ZU	SA	MM	EN
Bsp:	Preprocessed	HA	LX	LO	ZU	SA	MX	ME	NX
	Secret	AR	QU	UD	UV	...		

- Falls 2 auf gleicher Zeile: Beide Buchstaben um eins nach rechts
- Falls 2 auf gleicher Spalte: Beide Buchstaben um eins nach unten
- Falls 2 nicht auf gleicher Zeile/Spalte: Man nimmt die Buchstaben die auf seiner Spalte und auf des anderen Zeile liegen.
  $$\begin{array}{cccc} L & M & N & Q \\ \downarrow & & & \uparrow \\ U & V & W & X \end{array}$$

1.5 Koinzidenzindex (index of coincidence)

1. **Gegeben**
   Alphabet Alphabet $\mathcal{A} := \{A, B, C, \dots, Z\}$
   Sprache: Englisch
   $$\Rightarrow \text{Buchstabenhäufigkeit:} \quad \begin{array}{cccc} p_A & p_B & \cdots & p_Z \\ \shortparallel & \shortparallel & & \shortparallel \\ p_1 & p_2 & \cdots & p_3 \end{array}$$
   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: Was bedeutet $\boxed{IC_L := \sum_{1=1}^{26} P_i^2}$ **i**ndex of **c**oincidence L: Language

   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: $F = "AXCAABCXA"$
   $n_1 = \#A's$ in F
   $n_1 = \#B's$ in F
   $\vdots$

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

Definition $\boxed{IC_F = \frac{\sum_1^{26}\binom{n_i}{2}}{\binom{n}{2}}}$

Bsp:

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

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

Annahme $IC_F \xrightarrow[F\to\infty]{} IC_L$ (ist im Allgemeinen falsch)

Bemerkung

Permutation der Buchstaben
F $\mapsto$ Perm(F)
F = "AXCA..." $\mapsto$ Perm(F) = "CBYC..."
$\boxed{IC_F = IC_{Perm(F)}}$

1.6 Vigenères Chipres

1.6.1 Berechnung der Schlüssellänge eines Vigenère-Cipher

Gegeben

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

$$\overbrace{\begin{array}{|c|c|c|c|c|c|} \hline C_1 & C_2 & C_3 & C_4 & \cdots & C_p \\ \hline C_{p+1} & C_{p+2} & C_{p+3} & C_{p+4} & \cdots & C_{2p} \\ \hline C_{2p+1} & C_{2p+2} & C_{2p+3} & C_{2p+4} & \cdots & C_{3p} \\ \hline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hline C_{n-2} & C_{n-1} & C_n & - & - & - \\ \hline \end{array}}^{p}\left.\vphantom{\begin{array}{c}1\\1\\1\\1\\1\end{array}}\right\}\frac{n}{p}$$

$\uparrow \quad \nearrow \quad \nearrow$
monoalphabetisch

alle Spalten $= p$, alle Zeilen $= \frac{n}{p}$, letzte Zeile = monoalphabetisch!

$\alpha :=$ Anzahl Buchstabenpaare aus gleicher Spalte, $\alpha = \frac{n(\frac{n}{p}-1)}{2} = \frac{n(n-p)}{2p}$

$\beta :=$ Anzahl Buchstabenpaare aus verschiedenen Spalten, $\beta = \frac{n(n-\frac{n}{p})}{2} = \frac{n^2(p-1)}{2p}$

$\gamma :=$ Anzahl gleicher Buchstabenpaare aus C, $IC_L = \frac{\gamma}{\binom{n}{2}}$

$$\boxed{\gamma = \alpha \cdot IC_L + \beta \cdot IC_{\text{flat}}}$$

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

1.6.2 Kryptoanalysis des Vigenère-Cipher

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:

(i,j);k	0	1	2	$\cdots$	
$(1,2)$					
$(1,3)$					
$(1,4)$					
$(1,5)$					
$(2,3)$			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)
$MIC(s,t) = \frac{1}{kl}\sum_{i=1}^{26} n_i(s) n_i(t),\ |s| = k,\ |t| = l$
zb: $MIC(c_2, c_3{+}22 > 0.06 \iff c_2 \sim c_3 + 22 \Rightarrow \boxed{\beta_2 - \beta_3 = k}$

Notation s$\sim$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 $\iff c_i \sim c_j + k$

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

$\downarrow$ sind $\underline{\text{bekannt}}$

$$\left.\begin{array}{l} k_{12} = \beta_2 - \beta_1 \\ k_{13} = \beta_3 - \beta_1 \\ k_{52} = \beta_2 - \beta_5 \end{array}\right\}\text{Auflösen nach } \beta_1$$

Schlüsselwort: $\beta_1, \overbrace{\beta_2, \ldots, \beta_p}^{\text{abhängig von } \beta_1} = \beta_1, \beta_1 + k_{12}, \ldots,$

Ausprobieren: $\beta_1 = 0, 1, \ldots, 25$

1.7 One-Time-Pad

$$\Sigma = \{0,1\} \quad \begin{array}{ll} \text{Klartext:} & p_1p_2p_3p_4p_5\cdots = \\ \text{Schlüssel:} & k_1k_2k_3k_4k_5\cdots = \\ \text{ciphertext:} & \underset{p_1\oplus k_1}{c_1}\; c_2c_3c_4c_5\cdots = \end{array} \boxed{\begin{array}{c}0\\1\\1\end{array}} \begin{array}{l} 0101\ldots \\ 0110\ldots \\ 0011\ldots \end{array}$$

1.8 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

1.9 Kryptoanalysis

1.9.1 Ciphertext-only attack

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

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

1.9.2 known-plaintext attack

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

Gesucht k

1.9.3 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

1.9.4 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

$\Sigma = \{0, 1\}$
$\Sigma^n := \Sigma \times \Sigma \times \cdots \times \Sigma$

Definition

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

Bsp.

$n = 3$
$\Sigma^3 = \Sigma \times \Sigma \times \Sigma$

$$p \left\{ \begin{array}{ccc} 000 & \nearrow & 000 \\ 001 & \to & 001 \\ \dots & & \dots \\ 111 & \searrow & 111 \end{array} \right\} l$$

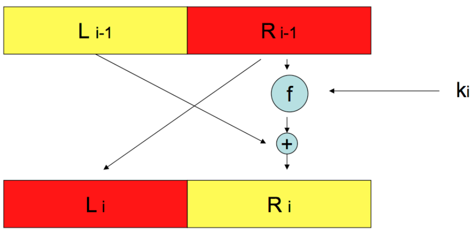
$\uparrow$Schlüssel

Frage:

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

2.1 Data Encription Standard (DES)

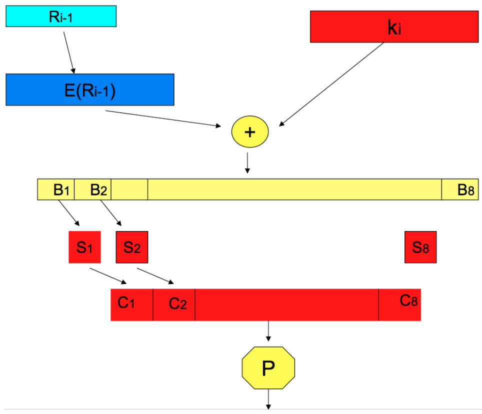
Lucifer	Schlüssellänge	128
$\downarrow$		
DES	Schlüssellänge	56
	Blocklänge	64



$$L_1 := R_0$$
$$R_1 := f(R_0, k_1) \oplus L_0$$

$$L_0 := f(L_1, k_1) \oplus R_1$$
$$R_0 := L_1$$

Die f-Funktion:



2.2 Modi von Block-Cipher

Sei $\Sigma := \{0, 1\}$
$p = c = \Sigma^4 = \{\square\square\square\square\}$
$k =$ Permutation von Σ^4
$k = \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Vor- und Entschlüsselung

Sei $m = 0101 \in p$ (Klartext)
$e_k(m) = e_k(0101) = 1010 = c$

2.2.1 ECB-Modus (electronic code block)

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

$\xrightarrow[m_1]{} \boxed{e_k} \xrightarrow[c_1]{}$

Bem:

1. $m_1 = m_3 \Rightarrow c_1 = c_3$
2. Vertauschen der Ciphertext-Blöcke wird nicht notwendigerweise erkannt

2.2.2 CBC-Modus (cipher block chaining)

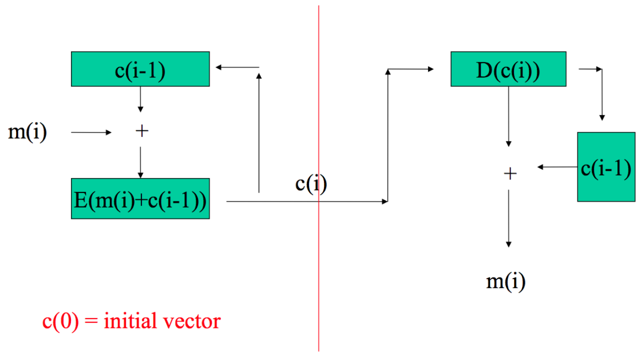
$m = \underset{\text{Länge n}}{m_1} |m_2| \dots, n$: Blocklänge

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

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

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

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



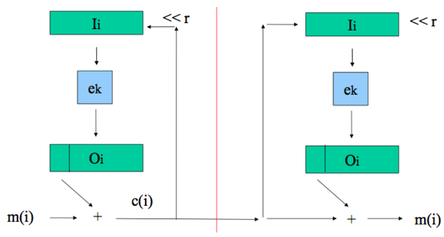
$m = \underbrace{m_1}_{\text{Länge n}} | m_2$, n : Blocklänge
IV =Initialvektor (i.a. bekannt)
$c_0 := IV$, $c_1 := e_k(c_0 \oplus m_1)$, $c_2 := e_k(c_1 \oplus m_2)$
$c_1 \oplus d_k(c_2) = d_k(e_k(c_1 \oplus m_2)) = c_1 \oplus m_2 \oplus c_1 = m_2$
Bsp: $m = \underbrace{1100}_{m_1} | \underbrace{0110}_{m_2} | \underbrace{1100}_{m_3} | 101$, $IV = c_0 = 1110$
$c_1 = e_k(c_0 \oplus m_1) = e_k(0010) = 0001$
$c_2 = e_k(c_1 \oplus m_2) = e_k(0111) = 1011$
$c_3 = e_k(c_2 \oplus m_3) = e_k(0111) = 1011$
Bem:

1. $m_1 = m_3 \not\Rightarrow c_1 = c_3$
2. Vertauschen kann bemerkt werden
3. Übertragungsfaktor machen sich bemerkbar

2.2.3 CFB-Modus (cipher feedback)

$m = \underbrace{\tilde{m}_1}_{\text{Länge}=r} | \tilde{m}_2 | \tilde{m}_3 | \ldots$, n: Cipher Block-Länge (DES: 64) und $\boxed{0 < r \le n}$

$I_1 \quad := IV \in \Sigma^n$
$\downarrow$
$\boxed{\text{DES}}$
$\downarrow$
$O_1 : \underbrace{\square}_{r} \; \square$
$\oplus \qquad \to c_1$
$\tilde{m}_1 \to \underbrace{\square}_{r}$



Bsp: $m = 110|001|101|100|101$, $IV = 1110$, $\boxed{r = 3,\ n = 4}$

$I_1 = 1110$
$\downarrow$
$\boxed{e_k}$
$\downarrow$
$O_1 \quad \mathbf{110}1$
$\oplus \qquad \to c_1 = 000$
$\tilde{m}_1 = 110$

$I_2 = \overbrace{111\mathbf{0}}^{I_1}\overbrace{\mathbf{000}}^{c_1}$
$\downarrow$
$\boxed{e_k}$
$\downarrow$
$O_2 \quad \mathbf{000}0$
$\oplus \qquad \to c_2 = 001$
$\tilde{m}_2 = 001$

3