Crypto 1 GÜ 6

17.) Theorem 4.13

„$\Rightarrow$" with Lemma 4.12.a.)

$$|\mathcal{M}_+| \le |C_+| \le |C| = |\mathcal{M}| \underset{\uparrow}{=} |\mathcal{M}_+|$$

$$P(\hat{M} = m) > 0 \ \forall m \in \mathcal{M}$$

$$\Rightarrow |C_+| = |C| \Rightarrow C_+ = C \Rightarrow P(\hat{C} = c) > 0 \ \forall c \in C$$

Let $m \in \mathcal{M}$, $c \in C$

$$0 < P(\hat{C} = c) \underset{\text{perf. secr.}}{=} P(\hat{C} = c \mid \hat{M} = m) = P(e(\hat{M}, \hat{K}) = c \mid \hat{M} = m)$$

$$\underset{\hat{M}, \hat{K} \text{ s.u.}}{=} P(e(m, \hat{K}) = c) = \sum_{k \in K : e(m,k) = c} P(\hat{K} = k) \neq 0$$

$$\Rightarrow \forall m \in \mathcal{M}, c \in C \ \exists k \in K : e(m,k) = c$$
(not unique)

Fix m: $|C_+| = |C| = |\{e(m,k) \mid k \in K_+ = K\}|$

$$\le |K| \underset{\text{Assumption}}{=} |C|$$

It follows that k is unique $k = k(m, c)$

Let $m \in \mathcal{M}$, $c \in C \Rightarrow P(\hat{C} = c) = P(\hat{K} = k(m, c))$

Cause of perf. secr. that is independent of m

Fix $C_0 \in \mathcal{C} \Rightarrow \{k(M, C_0) \mid M \in \mathcal{M}\} = \mathcal{K}$,

cause of injectivity of $e(\cdot, k)$
and the sets have same order $(|\mathcal{M}| = |\mathcal{C}|)$

$\Rightarrow P(\hat{C} = c) = P(\hat{K} = k) \quad \forall c \in \mathcal{C}, k \in \mathcal{K}$

$\Rightarrow P(\hat{K} = k) = \frac{1}{|\mathcal{K}|}$

<u>E19.)</u> For an affine cipher in $\mathbb{Z}_{26}$:

$e(i, (a,b)) = a \cdot i + b \mod 26$

$\mathbb{Z}_{26}^* = \{a \mid \gcd(a, 26) = 1\} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$\Rightarrow |\mathcal{K}| = |\mathbb{Z}_{26}^* \times \mathbb{Z}_{26}| = 12 \cdot 26$

Let $M \in \mathcal{M}$, $c \in \mathcal{C}$

$P(\hat{C} = c \mid \hat{M} = M) = P(e(\hat{M}, \hat{K}) = c \mid \hat{M} = M)$

$\hat{K}, \hat{M}$ st. indep.

$= P(e(M, \hat{K}) = c) = \frac{1}{|\mathcal{K}|} |\{k \in \mathcal{K} \mid e(M, k) = c\}|$

$\overset{(*)}{=} \frac{12}{12 \cdot 26} = \frac{1}{26}$

$(*)$: $e(M, (a,b)) = c \iff M \cdot a + b = c \pmod{26}$

$\iff b = c - aM \mod 26$

$\Rightarrow$ all keys $(a, c - aM \mod 26)$, $a \in \mathbb{Z}_{26}^*$ satisfy this equation

$\Rightarrow P(\hat{C} = c \mid \hat{M} = M) = \frac{1}{26} \quad \forall M \in \mathcal{M}_+$

Crypt 1 Bü 6

$$\Rightarrow P(\hat{C}=c) = \sum_{m \in \mathcal{M}_+} \underbrace{P(\hat{C}=c \mid \hat{M}=m)}_{\frac{1}{26}} \cdot P(\hat{M}=m)$$

$$= \frac{1}{26} = P(\hat{C}=c \mid \hat{M}=m)$$

$\Rightarrow$ $\hat{C}$ and $\hat{M}$ are sto. indep.

$\Rightarrow$ Cor 4.11. the crypto system has perfect secrecy.

<u>E 18.)</u> <u>Recall</u>: $H(X) = -\sum_i P_i \log(P_i)$

a.) $H(\hat{M}) = -\frac{1}{4} \log_2(\frac{1}{4}) - \frac{3}{4} \log_2(\frac{3}{4}) = \frac{1}{2} + \frac{3}{2} - \frac{3}{4}\log_2(3)$

$\approx 0{,}811$

$H(\hat{K}) = -\frac{1}{2} \log_2(\frac{1}{2}) - 2 \cdot \frac{1}{4} \log_2(\frac{1}{4}) = \frac{1}{2} + 1 = \frac{3}{2} = 1{,}5$

$c = e(m,k)$	k_1	k_2	k_3	
$m = a$	1	2	3	1/4
$m = b$	2	3	4	3/4
	1/2	1/4	1/4	

$P(\hat{C}=1) = P(\hat{M}=a) \cdot P(\hat{K}=k_1) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

$P(\hat{C}=2) = P(\hat{M}=a) \cdot P(\hat{K}=k_2) + P(\hat{M}=b) \cdot P(K=k_1)$

$= \frac{1}{4} \cdot \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{2} = \frac{7}{16}$

$P(\hat{C}=4) = P(\hat{M}=b) \cdot P(\hat{K}=k_3) = \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}$

$P(\hat{C}=3) = 1 - P(\hat{C}=1) - P(\hat{C}=2) - P(\hat{C}=3) = 1/4$

$H(\hat{C}) = -\frac{1}{8} \log(\frac{1}{8}) - \frac{7}{16} \log(\frac{7}{16}) - \frac{3}{16} \log(\frac{3}{16}) - \frac{1}{4} \log(\frac{1}{4})$

$\approx 1{,}85$

$H(\hat{K} \mid \hat{C}) \underset{Th. 4.7.}{=} H(\hat{M}) + H(\hat{K}) - H(\hat{C}) \approx 0{,}461$

b.) It is $4 = |C_+| > |K_+| = 3$ ↯ Lemma 4.12.b.) $|C_+| \leq |K_+|$

c.) Variant 1: Apply Th. 4.13.

(i) $P(\hat{K} = K_i) = \frac{1}{3} > 0$

(ii) $C = \{1, 2, 3\}$

(iii) $M = \{a, b, c\}$ $P(\hat{M} = c) = 0$

Remark 4.14: $\hat{M}, \hat{C}$ are still st. indep.

$e(M,K)$	K_1	K_2	K_3
a	1	2	3
b	2	3	1
c	3	1	2

$\Leftrightarrow \forall M, c\ \exists! K$ with $e(M,K) = c$

Variant 2.)

$e(M,K)$	K_1	K_2	K_3	K_4
a	1	2	3	4
b	2	3	4	1
	1/4	1/4	1/4	1/4

$P(\hat{C} = c) = 1/4$

$P(\hat{M} = M \mid \hat{C} = c) = P(\hat{M} = M) \Rightarrow \hat{C}, \hat{M}$ are st. indep.

$\underset{cor. 4.11.}{\Rightarrow}$ perf. secr.