AARHUS UNIVERSITY - COMPUTER SCIENCE DEPARTMENT

Crypthology - Handin 3

Peter Burgaard - 201209175

September 21, 2016

1 CRYPTO SYSTEMS - PROBLEM 2

2 STINSON - 2.12

Prove that, in any cryptosystem $H(K|C) \geq H(P|C)$

Basicly we have to prove $H(K|C) - H(P|C) \geq 0 \implies H(K|C) \geq H(P|C)$. The proof is as follows

Proof.

By Stinson theorem 2.10

$$H(K|C) - H(P|C) = H(K) + H(P) - H(C) - H(P|C)$$

From the proof section of 2.10 have

$$H(K,P,C) = H(K,P) = H(K) + H(P)$$

Which implies

$$H(K) + H(P) - H(C) - H(P|C) = H(K,P,C) - H(C) - H(P|C)$$

By theorem 2.8

$$H(K,P,C) - H(C) - H(P|C) = H(K,P,C) - H(P,C)$$

Again by theorem 2.8

$$H(K,P,C) - H(P,C) = H(K|P,C)$$

Since entropy can never be negativ, we get

$$H(K|C) - H(P|C) = H(K|P,C) \geq 0$$

$\square$

3 Stinson - 2.14

Compute $H(K|C)$ and $H(K|P,C)$ for the *Affine Cipher*, assuming that keys are used equiprobably and the plaintext are equiprobable.

Since $|\mathscr{P}| = 26$, and the letters are equiprobably chosen, we get from Stinson p. 55

$$H(P) = log_2(|\mathscr{P}|) = log_2(26) \approx 4.7$$

Since a key K is a pair (a,b), where $a,b \in \mathbb{Z}$ and $gcd(a,26) = 1$, we have 26 different b's and $\phi(26) = 12$ a's. This implies 312 different, keypairs, which, again, are equiprobably chosen:

$$H(K) = log_2(|\mathscr{K}|) = log_2(312) \approx 8.285$$

Becuase the plain text and the key are equiprobably chosen, and affine uniquely encodes every $x \in \mathscr{P}$ to $e_K(x) = y \in \mathscr{C}$ we see that, the probability of y is the same as x, which implies:

$$H(C) = H(P) \approx 4.7$$

This gives us by theorem 2.10, Stinson:

$$H(K|C) = H(K) + H(P) - H(C) = H(K) \approx 8.285$$

By exercise 2.12 Stinson, and theorem 2.8

$$H(K|P,C) = H(K|C) - H(P|C) \approx 8.285 - 4.7 \approx 3.584$$