IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises IV.

1. Let $\mathcal{C}$ be a cryptosystem with plaintext space $P = \{x, y, z\}$, key space $K = \{k_1, k_2, k_3\}$ and cryptotext space $C = \{a, b, c\}$.
   The probability distributions p_P and p_K are defined as

   $$p_P(x) = \frac{3}{8},\ \ p_P(y) = \frac{1}{8},\ \ p_P(z) = \frac{1}{2};$$

   $$p_K(k_1) = \frac{1}{3},\ \ p_K(k_2) = \frac{1}{6},\ \ p_K(k_1) = \frac{1}{2}.$$

   The encryption function is given by the following table:

	x	y	z
k_1	a	b	c
k_2	b	c	a
k_3	c	a	b

   (a) Determine the probability distribution p_C.

   (b) Is $\mathcal{C}$ perfectly secure? Explain your reasoning.

2. Decrypt the following ciphertexts.

   (a) `AABCCEEHHIILLOPPPRTY`

   (b)
   ```
   TEGUN LRNCS XXXIJ GJCPV CYMOA QUSKL UWMCJ
   CWKIN NGNPZ JIIML MGVCS ZRJIX UCRRR ROWSY
   WKSJA YNLRC AMTSB OQAEM WIIIJ SAFGS XXEUW
   VPEQV PUNXR TMKKL UEILG YHYGE FYZPA TEWYM
   XFQDU CEYHX RZRYY EJBEF DCJEI DWVLR RJUFO
   UWVPE QVGQY WNTAN GLULX UGAFV WQLOR AGXAY
   INXUG JJKXU LSSVF JMMWY RRTCP VCJBE GYYXL
   WUXJB TRMRX SIPHO LZJMD AQRVF TUWIC QVNYW
   KSJBS FGSXV HJIFE GYPKL UWERU YWTMF BIEVF
   JCIJN IEUGS KLUWM CJCWK INNGN PZJUM IWSIG
   PJU
   ```

   (c)
   ```
   ABABB ABABA ABAAB AAAAA ABBAB
   BABAA BBBBB ABAA
   ```

   (d) `JZDGCVVOVITZJV`

3. You have found an old cryptotext encrypted with the Vigenere cryptosystem. You have observed that the cryptotext contains three occurrences of the sequence CGIRTFGH. These occurrences start at positions 37, 1283 and 2354. What can you deduce about length of the key?

4. Let $\mathcal{C}$ be a product cryptosystem which consists of two transposition cryptosystems whose block sizes are m and n. Determine the block size of $\mathcal{C}$. Explain your reasoning.

5. Let $\mathcal{C} = (P, C, K, e, d)$ be a cryptosystem.

   (a) Suppose that $\mathcal{C}$ is perfectly secure. Show that for any $m \in P$ and $c \in C$ it holds that $Pr(C = c|P = m) = Pr(C = c)$.

   (b) Suppose that for any $m, m' \in P$ and $c \in C$ it holds that

   $$Pr(P = m|C = c) = Pr(P = m'|C = c).$$

   Show that C is perfectly secure.

6. Let S be an endomorphic cryptosystem. Let $S^2 = S \times S$. Which of the following simple cryptosystems – the Shift, Vigenere, Hill or Affine cryptosystem – would you prefer to use as S^2. Explain your reasoning.

7. What is the number of keys one can use in the Hill cryptosystem with matrices of degree 2 over $\mathbb{Z}_{26}$?