IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises IV.

1. Consider a sequence of $n \in \mathbb{N}$ Affine ciphers. Let (a_i, b_i) be the key of the i-th cipher. Show that if Alice encrypts her message m using this sequence of ciphers, she obtains a cryptotext encrypted by a single Affine cipher. Determine the key (a, b) of this cipher.

2. You know that the following cryptotext was created using the Vigenere cryptosystem and the corresponding plaintext is part of the article about numbers. Try to find the original message or at least determine the keylength.

   ```
   CZWCW NSPCX HMOXY KDOVE GXIPC DSPKC ELCVK MTSXF OPSPI ORCTK XGPQE
   QGAYC PMIMH XYKDO VQVRE RCZTP QHMKC DIQVR INTYT CTDMC UYJPC XHMOX
   YKDOV Q
   ```

3. Eve intends to perform a chosen plaintext attack on

   a) a shift cryptosystem,

   b) a transposition cryptosystem with a block size $k \leq 26$,

   c) a simple substitution cryptosystem,

   d) Vigenere cryptosystem with a key of known length d.

   Since Eve is lazy, she wants her attacks to be as efficient as possible. For each cryptosystem determine the length of the shortest plaintext which enables her to completely determine the key.

4. Alice wants to send an encrypted message to Bob but she knows only the Playfair and Affine cryptosystems.
   Is it more secure to encrypt a message first using the Playfair, then Affine and finally again with the Playfair cryptosystem or to encrypt a message with just the Playfair cryptosystem? Explain your reasoning.

5. Decide whether the following cryptosystems are perfectly secure. Explain your reasoning. In both cases each key is used with the same probability.

   a) $P = C = K = \mathbb{Z}_7$, $e_k(m) = m + k^4 \pmod 7$

   b) $P = C = K = \mathbb{Z}_7$, $e_k(m) = m + k^5 \pmod 7$

6. Decrypt the following cryptotexts (continued on next page).

   a) `PNRFNEPELCGBFLFGRZ`

   b) `SEPCFAYRRTOTAMALS`

   c) `CJCICFEIAGBIDJDH`

   d) (Keyword = PASSWORD)

   ```
   LE ZL IK WO GS NO MO MB ON KB ZK ON PK BZ OR CF BT ER
   ```

e) GEOGRAPHY ANTS
MARKETING WAR

f) XQFXMGAFFDSCHFZGYFZRSHEGHXQZXMFQRSPEGHXQKPZNKZGHGNGHX
QDEEFDSZHQGAFVDJDZNGSDDGFIGBSHGGFQHQGAF4GARFQGNSPDYKP
GAFKSDAJHQZRAXCDSUDGZPDPDQDKNGKDZFYXQJDQNZRSHEGZYDGHQ
TKDRVGXGAF4GARFQGNSPKRGAFVDJDZNGSDSFRXJJFQYZGADGBXJFQ
ZAXNCYZGNYP64DSGZHQRCNYHQTRXXVHQTYSFZZHQTJDZZDTFDQYGA
FESFEDSDGHXQXMEFSMNJFZGAFCHZGDCZXHQRCNYFZZXJFCFZZXKUH
XNZDSGZHQRCNYHQTRXQONSHQTRAFZZKXXVKHQYHQTDQYRDSEFQGSP
QNJKFS45XQGAFCHZGHZJCFRRAHGDUHVDCEDGAFDSGXMZFRSFGBSHG
HQTDYUXRDGFYHQXSYFSGXAFCEBXJFQRXQRFDCGAFYFGDHCZXMGAFH
SCHDHZXQZXQFXMGAFSFRXJJFQYFYGFRAQHLNFZHQUXCUFZSDQYXJC
PEDHSHQTCFGGFSZXMGAFDCEADKFGDQYGAFQZNKZGHGNGHQTFDRACF
GGFSHQGAFXSHTHQDCJFZZDTFBHGAHGZEDSGQFS

7. *(Bonus Exercise)* You have captured a messenger with the message written below. The messenger had two things: a box with 154 pebbles and "Avisa Relation oder Zeitung". Use this two pieces of evidence to decrypt the message.

154 5 23 2 11 1 42 3 65 4 71 1 88 3 95 3 101 2 107 2 46 3