

## 2007 - Exercises IV.

1. Decode the following cryptotexts:

- (a) AMICABLE PHOTON
- (b) START OPINIONS
- (c) KTZWYMJCJWHNXJ
- (d)  $a^3e^3i^3n^2op^2s^2t^4$

2. A simple substitution cipher  $f : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$  (a plaintext letter  $x$  is substituted with a cryptotext letter  $f(x)$ ) is called self-inverting if  $f(x) = f^{-1}(x)$ , *ie.*  $f(f(x)) = x$ .

- (a) How many different self-inverting substitution ciphers are there?
- (b) What is the proportion of self-inverting substitution ciphers to all simple substitution ciphers?
- (c) How many self-inverting substitution ciphers which do not map any letter onto itself are there?

3. Decrypt the following cryptotext which was obtained using the Vigenere cryptosystem.

CTWIJ NSDVF KBJXZ GTXRV CAHRL CZVSX EWSLW TGWLW TSDVW  
OOQCK JCUXU WHVXG DSOIS TBHHA PCUHW THRFW ECPIU KDKIJ  
GLSIJ VGWLW USVEN GHLQW CBGEV FHRS M TSQNG AAHRL

4. Try to decode the following cryptotext. You know that the one-time pad cryptosystem (using addition modulo 26) was used and the encryption key starts with “GSC”.

GLUYM YIFGH EJPCR OFLSM DOFML QSFCD F MZHLL VDJLE  
TTYNM XDKEC ALIOP DHTFN ECRKF GKDV RJ DJVMR WICKF

5. Decide whether the following cryptosystems are idempotent. Explain your reasoning.

- (a) the Caesar shift cipher;
- (b) the Affine cipher;
- (c) the Hill cipher;
- (d) the Vigenere cipher.

6. Encrypt the word “cryptology” with
  - (a) the Polybius square cryptosystem;
  - (b) the Hill cryptosystem with  $M = \begin{pmatrix} 6 & 7 \\ 3 & 11 \end{pmatrix}$ ;
  - (c) the Caesar cryptosystem with  $k = 6$  and the keyword “SHIFT”;
  - (d) the Autoclave cryptosystem with the keyword “KEY”.
7. Assume that the Affine cryptosystem is implemented in  $\mathbb{Z}_{126}$ .
  - (a) Determine the number of possible keys.
  - (b) For the encryption function  $e(x) = 23x + 7 \pmod{126}$  find the corresponding decryption function.
8. (*Bonus Exercise*) You have found an old-looking parchment with the following text:

20 4 22 8  
 42 22 71 8  
 36 3 7 11  
 38 6 6 2  
 2 26 17 8  
 66 5 1 22  
 19 80 9 3  
 14 32 7 1  
 45 14 14 13  
 4 29 20 6

1566–1625, 1611