Číslo cvičení: 4
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. (a) ROSICRUCIAN CIPHER
   (b) POLYBIUS SQUARE
   (c) Playfair cipher with keyword PLAYFAIR results WHEATSTONE.

2. (a) $|P| = |K| = |C| = 26$ and for this system the theorem on p. 46 of the slides holds $\implies$ it is perfectly secure.
   (b) There are 26! different monoalphabetic subtitutions $\implies |P| \leq 26!$. Let $P$ be all permutations of the word ab...z $\implies |P| = 26!$. For every $w \in P, c \in C$ there is exactly one $k \in K$ such that $e_k(w) = c$, because we do not repeat characters in any of $c, w, k$ and exhaust all permutations. If we choose all the keys with equal probabilities, the same theorem as in (a) holds $\implies$ the maximum cardinality is 26!.
   (c) If the length of the keyword is also $n$, all keywords are used with the same probability, then it is a one-time-pad cipher, which is perfectly secure.

3. The only solution is $f = 1$. For every other $f$ exists $k \neq 0$ such that $k^f = 0$ which breaks the perfect security.

4. THE IDEALS WHICH HAVE LIGHTED MY WAY AND TIME AFTER TIME HAVE GIVEN ME NEW COURAGE TO FACE LIFE CHEERFULLY HAVE BEEN KINDNESS BEAUTY AND TRUTH THE TRITE SUBJECTS OF HUMAN EFFORTS POSSESSIONS OUTWARD SUCCESS LUXURY HAVE ALWAYS SEEMED TO ME CONTEMPTIBLE
   Affine cipher $a = 11, b = 3$. V and E are the most common in the cryptotext and were on first try transformed to E and T.

5. We get two equations:
$$24 \equiv 11a + 4b + 5 \mod 26$$
$$15 \equiv a + 17b + 9 \mod 26$$
   There is one solution $a = 24, b = 15$, the plaintext is $\binom{24}{15}$.

6. $1423-91 = 1332, 1819-1423 = 39$, $\gcd(1332, 396) = 36 \implies$ possible key lengths are: 36,18,12,9,6,3,2,1.

7. (a)
   (b) 1984 Bible code, The Magic Words are Squeamish Ossifrage
   (c) "securitythroughobscurity", however the cipher is highly ambiguous.
   (d) The system must be practically, if not mathematically, indecipherable;
   It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
   Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
   It must be compatible with the means of communication;
   It must be portable, and its usage and function must not require the concourse of several people;
   Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.