

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

1. (a) ROSICRUCIAN CIPHER
(b) POLIBIOUS SQUARE
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)
(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.
- 6.
7. (a)
(b)
(c) securitythrouiobscurity
(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.