Department of Applied Mathematics and Computational Sciences

MSc - Theoretical Computer Science (VI Sem)

15XT68 - Security in Computing Laboratory

PROBLEM SHEET 1

1. Decipher WZUSAAL if the encipherment function is E(x) = (5x + 8) MOD 26 (affine cipher)

2. Below is ciphertext produced by an affine cipher with undisclosed encryption key. Try to decrypt it using exhaustive search. (x must have a gcd of 1 with 26)

OYHYJLEVYQBLSRIJLYEC

3. Implement the Playfair Cipher for enciphering and deciphering messages. Input data will come from files.

Text to be enciphered will be arbitrary text. It will be mixed case, with spaces and punctuation marks. The output will be all lowercase; letters will be in blocks of 5, starting in the leftmost column, with a single space between blocks (the last block may contain fewer than 5 characters); and there will be ten blocks per line (the last line may have fewer blocks).

Example :

Plain text:

An anonymous reader sends word of a proof-of-concept Google Chrome browser extension that steals users' login details. The developer, Andreas Grech, says that he is trying to raise awareness about security among end users, and therefore chose Chrome as a test-bed because of its reputation as the safest browser.

Example ciphertext output (to the console):

fafaw aermw yqnvm vqyns genwm hwoln kqwow ofkpf nexcq wqfvp
dckqu vhzwn ynmyz unsig wazcl wpxnv ipxey mpiqf asmvw lbvpx
dymvd vaken obefm yinhq pdgyb npxfb zcsvp xzbas cxqki bynfn
bonsn yniar wuynd tqbzp vowad sefxe ymnie fzcym ndqkp dfryn
dckqu vinlw nyzlv mvyfl xenmg axpmy etwlx lwain zcnyf onyzl
kqxny m