Mathematics Department, University of Massachusetts Dartmouth

Discrete Mathemtics II

MTH182 – Section 03 – Spring 2015

Problem set 9

Cryptography

Reading:	Discrete Mathematics, first edition, section Sections 7.5 Section 7.5: 1, 3, 5, 7, 9

Section 7.5

1. Encrypt the message "YOU ARE CORRECT SIR" by transforming letters into integers using the encryption function defined by $f(x) = (x + 5) \bmod 26$ for $x \in \mathbb{Z}$, $0 \leq x \leq 25$.

3. Using a certain Caeser cipher, a message is transformed into the secret message "LIPT MW LIVI". What is the original message?

5. Consider the cryptosystem in which the integer x associated with a letter is transformed into $f(x) = 3x \bmod 26$. In this case, decryption is defined by $f^{-1}(x) = 9x \bmod 26$.

(**a**) Into which secret word is the word GUM transformed?

(**b**) Which word is transformed into the secret word FOYN?

(**c**) Which word is transformed into the secret word JAN?

7. It is decided to have a cryptosystem in which the integer x associated with a letter is transformed into $f(x) = 2x \bmod 26$. Why is this a bad idea?

9. Consider the cryptosystem in which the integer x associated with a letter is transformed into $f(x) = x + (-1)^x$ for $x \in \{0, 1, \ldots, 25\}$.

(**a**) Which word is transformed into the secret word BAPUF?

(**b**) Determine f^{-1}.