CS 327 PA1

James Tremblay

September 2024

Excersize 7.1

[**7.1**] **Using what you have learned about modular arithmetic, solve for the decryption function D(c, a, b) which equals m when c = E(m, a, b). Once you have solved for the function D(c, a, b) answer the following questions.**

1. **What is the decryption function** $D(c, a, b)$**?**

$$
\begin{aligned}
c &\equiv (a \times m + b) \textbf{ mod } 128 \\
c - b &\equiv a \times m \textbf{ mod } 128 \\
\frac{(c-b)}{a} &\equiv m \textbf{ mod } 128 \\
(c-b) \times a^{-1} &\equiv m \textbf{ mod } 128 \qquad\qquad \textbf{gcd(a, 128) = 1}
\end{aligned}
$$

   Therefore the decryption function $D(c, a, b)$ **is...**
   $m \equiv (c - b) \times a^{-1}$ **mod** 128**.**

2. **Are all choices of integers** (a, b) **valid keys? In other words, does** $D(c, a, b)$ **exist for all possible choices of** (a, b)**? If not, what restrictions must be placed on** a **and** b **to ensure that the decryption function exists?**

   All choices of integers (a, b) **are not valid keys.** a **must be relatively prime to** 128**, otherwise it would not have a modular inverse and therefore would not be able to cover all possible characters in the ASCII model.** b **has no restrictions on it as it is the shift value, however it makes the most sense for** $0 \leq b \leq 127$**.**

3. Give a reasonable upper bound on the number of different key pairs (a, b) that can be used to encrypt ASCII text. (HINT: remember that when you are doing modular arithmetic with modulus 128, you are really (in a sense) working with the residue classes $[0]_{128}, ..., [127]_{128}$.

There are 128 potential values that b could be. For a the number has to be relatively prime with 128, therefore they cannot share any numbers in the prime factorization of both. The prime factorization of 128 is 2^7. This means that any integer, p such that $0 \leq p \leq 127$ with a 2 in the prime factorization cannot be a possible value for a. This means that there are 64 possible values for a as it is every odd number in that range.
As there are 128 possible values of b and 64 possible values of a Therefore there are $128 \times 64 = 8192$ possible key pair combinations of a and b.