Solutions to
Applied Cryptography (Version 0.6, Jan. 2023)
by Boneh & Shoup

Edgard Lima <edgard.lima@gmail.com>
https://edgardlima.com

2025

Contents

Chapter 2

Encyption

1.1 (multiplicative one-time pad). We may also define a "multiplication mod p" variation of the one-time pad. This is a cipher E = (E, D), defined over (K, M, C), where K := M := C := 1, . . . , p-1, where p is a prime. Encryption and decryption are defined as follows:

$$E(k, m) := k \cdot m \bmod p \qquad D(k, c) := k^{-1} \cdot c \bmod p$$

Here, k^{-1} denotes the multiplicative inverse of k modulo p. Verify the correctness property for this cipher and prove that it is perfectly secure.

Answer: Auxiliary

Notice that $k^{-1} \cdot k \bmod p = 1$ (multiplicative inverse of k modulo p)

Given p is prime, k^{-1} is unique. Let's prove.
Suppose there is x and y, such that $k \cdot x \bmod p = 1 = k \cdot y \bmod p$. Also, make sure x and y are reduced by mod$p$. *i.e.* $0 < x, y < p$
Since p is prime and $0 < k < p$, we can divide both sides by k.
$x \bmod p = y \bmod p$
$x = y$

Answer: Correctess

Notice that $k^{-1} \cdot k \bmod p = 1$ (multiplicative inverse of k modulo p)

$c = Enc(k, m) := k \cdot m \bmod p$
$Dec(k, Enc(k, m)) = k^{-1} \cdot c \bmod p$
$Dec(k, Enc(k, m)) = k^{-1} \cdot (k \cdot m \bmod p) \bmod p$
$Dec(k, Enc(k, m)) = k^{-1} \cdot k \cdot m \bmod p \bmod p$
$Dec(k, Enc(k, m)) = k^{-1} \cdot k \cdot m \bmod p$
$Dec(k, Enc(k, m)) = 1 \cdot m \bmod p$
Since $1 \leqslant m \leqslant p - 1$, then
$Dec(k, Enc(k, m)) = m$

Answer: Perfectly Secure

$m^{-1} \cdot m \bmod p = 1$ (multiplicative inverse of m modulo p)

$k \cdot m \bmod p = c$
$k \cdot m \cdot m^{-1} \bmod p = c \cdot m^{-1} \bmod p$
$k \bmod p = c \cdot m^{-1} \bmod p$
Since m^{-1} is unique, for every $c \in \mathcal{C}$, and for all message $m \in \mathcal{M}$
$N_c = |\{k \in \mathcal{K} : E(k, m) = c\}| = 1$
This is perfectly secure according to **Theorem 2.1 (ii)**