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

Edgard Lima <edgard.lima@gmail.com>

https://www.linkedin.com/in/edgardlima/

https://edgardlima.com

https://github.com/Zer0Leak/AppliedCryptographyBonehBookSolutions

2025

Contents

Chapter 2

Encyption

2.1 (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 $\bmod p$. $i.e.$ $0 < x, y < p$
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)**

2.2 (A good substitution cipher). Consider a variant of the substitution cipher $\mathcal{E} = (E, D)$ defined in Example 2.3 where every symbol of the message is encrypted using an independent permutation. That is, let $\mathcal{M} = \mathcal{C} = \Sigma^L$ for some a finite alphabet of symbols Σ and some L. Let the key space be $\mathcal{K} = S^L$ where S is the set of all permutations on Σ. The encryption algorithm E(k, m) is defined as:

$$E(k, m) := k[0](m[0]), k[1](m[1]), ..., k[L-1](m[L-1])$$

Show that $\mathcal{E}$ is perfectly secure.

Answer

The encryption decryption of each symbol is independent. At each index there is an independent **substitution cipher**.

Therefore, we can reduce to prove that $\mathcal{M} = \mathcal{C} = \Sigma$, and $\mathcal{K} = S$, *i.e.*, m and c has length 1, and $|\mathcal{K}| = |\Sigma|!$ is perfectly secure.

$P_r[Enc(k, m) = c] = P_r[k(m) = c] = 1/|\Sigma|$ for all $m \in \mathcal{M}$ and all $c \in \mathcal{C}$ and an uniform distribution of $\mathcal{K}$

Therefore it is perfectly secure directly from the **Definition 2.1 (perfect security)**

2.3 (A broken one-time pad). Consider a variant of the one time pad with message space $\{0,1\}^L$ where the key space $\mathcal{K}$ is restricted to all L-bit strings with an even number of 1's. Give an efficient adversary whose semantic security advantage is 1

Answer

The adversary, $\mathcal{A}$, choose $m_0 := 0^L$, and $m_1 := 0^{L-1}1$

If the cipher text c has an even parity it outputs $\hat{b} = 0$ (because it was exactly the parity of the key)

Otherwise, cipher text c has an odd parity, it outputs $\hat{b} = 1$. Because the number of 1's will be the number of 1's in the key, that is even, minus one if the key has a 1 at index $L - 1$, or plus one, if the key has a 0 at index $L - 1$.