TCSS 581 Cryptology

Homework 2

Tianyi Li
Student ID: 1827924

Tianyi Li
Student #:1827924

2.1 Prove the second direction of Lemma 2.2.

An encryption scheme (Gen, Enc, Dec) over a message space M is perfectly secret if and only if for every probability distribution over M, every message *m* ∈ *M, and every ciphertext c* ∈ *C:*

Pr [*C = c* | *M = m*] = Pr [*C = c*].

- Second direction, given the scheme *E = (Gen, Enc, Dec)* is perfectly secret:
  - Let the key space be *K*, the message space be *M*, and the ciphertext space be *C*.
  - Since the scheme is perfectly secret,
  - Then Pr [*M = m* | *C = c*] = Pr [*M = m*], by Definition 2.3 from textbook V2.
  - Using the Bayes' theorem:

Multiply both sides with $Pr[C = c]$

$$Pr[M = m | C = c] = Pr[M = m]$$

$$Pr[M = m | C = c] \times Pr[C = c] = Pr[M = m] \times Pr[C = c]$$

$$\frac{Pr[M = m | C = c] \times Pr[C = c]}{Pr[M = m]} = \frac{Pr[M = m] \times Pr[C = c]}{Pr[M = m]}$$

Divide both sides with $Pr[M = m]$

$$\frac{Pr[M = m | C = c] \times Pr[C = c]}{Pr[M = m]} = Pr[C = c]$$

$$Pr[C = c | M = m] = Pr[C = c]$$

- Thus, given the scheme is perfectly secret, Pr [*C = c* | *M = m*] = Pr [*C = c*].

2.2 Prove or refute: For every encryption scheme that is perfectly secret, it holds that for every distribution over the message space *M*, every *m, m'* ∈ *M. and* every *c* ∈ *C:*

Pr [*M = m* | *C = c*] = [*M = m'* | *C = c*].

- Refute. This statement is false.
- Counter example:
  - With this encryption scheme *E = (Gen, Enc, Dec)*.
  - Let the key space be *K*, the message space be *M = {a, b}*, and the ciphertext space be *C*.
  - Consider an non-uniform distribution where Pr [M = a] = $\frac{1}{4}$, and Pr [M = b] = $\frac{3}{4}$.
  - Then *Dec* will return *a* on input ciphertext *0,* and *b* on input ciphertext *1*.
  - Thus Pr [M = a | C = c] = Pr [M = a] = $\frac{1}{4} \neq \frac{3}{4}$ = Pr [M = b] = Pr [M = b | C = c].
- Therefore, this scheme is not correct.

2.3 When using the one-time pad (Vernam's cipher) with the key $k = 0^{\ell}$, it follows that $Enc_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^{\ell}$, (i.e., to have *Gen* choose *k* uniformly from the set of non-zero keys of length *l*). Is this an improvement? In particular, is it still perfectly secret? Prove your answer.

- The new scheme is not perfectly secret.
- Since in this case, the message space will be larger than the key space.
- Consider an uniform distribution where $M = \{0, 1\}^{\ell}$, with messages $a = \{0, 1\}^{\ell}$.
- Then Pr [M = a | C = a] = 0 ≠ Pr [M = a].
- From the textbook and by the One-Time Pad definitions, in order to achieve perfect secrecy, it uses the key 0^{ℓ} to encrypt.
- But this proposed method seems to break that definitions down, since the keys would not be able to encrypt plaintext now.
- However, if the adversary does not know the fact that the key is 0^{ℓ}, then the ciphertext (which is also the plaintext, since it could not was not able to be encrypted) does not help the adversary as well.

2.5 Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

- Refute. This statement is false.
- Counter example:
  - Consider an encryption scheme *E = (Gen, Enc, Dec).*
  - Let the key space be *K*, the message space be *M*, and the ciphertext space be *C*, such that *K = M = C,* and $Enc_k(m) = m$, for every $m \in M$ and every $k \in K$.
  - Let $M = \{a, b\}$, $k = \{k_1, k_2\}$, $C = \{0, 1\}$.
  - Let $Enc_k(a) = 0$, $Enc_k(b) = 1$ for $k = k_1, k_2$.
  - Then *Dec* will return *a* on input ciphertext *0,* and *b* on input ciphertext *1*.
  - Thus Pr [M = a | C = 1] = 1 ≠ 0 = Pr [M = b | C = 1].
- Therefore, this scheme is not perfectly secret.