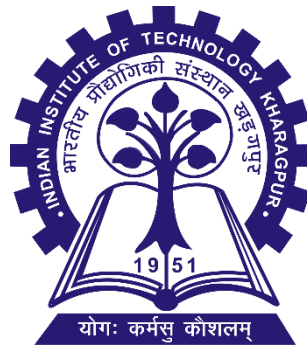


Cryptography and Network Security (CS60065) AUTUMN, 2023-2024

TA: Tapadyoti Banerjee

**Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India**



**TUTORIAL: 2
DATE: 6th September 2023**

The Entropy

Suppose X is a discrete random variable that takes on values from a finite set X . Then, the entropy of the random variable X is defined to be the quantity

$$H(\mathbf{X}) = - \sum_{x \in X} \Pr[x] \log_2 \Pr[x]$$

QUESTION : 1 (The Entropy)

Let $P = \{a, b\}$ with $\Pr[a] = 1/4$, $\Pr[b] = 3/4$. Compute $H(P)$.

Let $K = \{K1, K2, K3\}$ with $\Pr[K1] = 1/2$, $\Pr[K2] = \Pr[K3] = 1/4$. Let $C = \{1, 2, 3, 4\}$, and the cryptosystem can be represented by the following encryption matrix:

	a	b
K1	1	2
K2	2	3
K3	3	4

The Entropy

Suppose X is a discrete random variable that takes on values from a finite set X . Then, the entropy of the random variable X is defined to be the quantity

$$H(\mathbf{X}) = - \sum_{x \in X} \Pr[x] \log_2 \Pr[x]$$

Reading Assignment:

THEOREM 3.6 *Suppose \mathbf{X} is a random variable having a probability distribution that takes on the values p_1, p_2, \dots, p_n , where $p_i > 0, 1 \leq i \leq n$. Then $H(\mathbf{X}) \leq \log_2 n$, with equality if and only if $p_i = 1/n, 1 \leq i \leq n$.*

THEOREM 3.7 *$H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y})$, with equality if and only if \mathbf{X} and \mathbf{Y} are independent random variables.*

QUESTION : 2 (The Key Equivocation)

Let (P, C, K, E, D) be a cryptosystem. Then prove the followings:
 $H(K|C) = H(K) + H(P) - H(C)$.

The Spurious Keys and Unicity Distance

The Spurious Keys and Unicity Distance

Reading Assignment:

- 1) Prove a bound on the expected number of spurious keys.
- 2) **THEOREM 3.11** *Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem where $|\mathcal{C}| = |\mathcal{P}|$ and keys are chosen equiprobably. Let R_L denote the redundancy of the underlying language. Then given a string of ciphertext of length n , where n is sufficiently large, the expected number of spurious keys, \bar{s}_n , satisfies*

$$\bar{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1.$$

QUESTION : 3 (Quadratic Residue)

Find the quadratic residues and quadratic non-residues in \mathbb{Z}_{11}

QUESTION : 4 (Congruence)

Let g be a primitive root for \mathbb{F}_p . Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h \pmod{p}$. Prove that $a \equiv b \pmod{p - 1}$.

QUESTION : 5 (\mathbb{Z}_p^* and cyclic group)

Suppose $p = 13$. Find how many primitive elements are there in modulo 13.
And, examine it for 2.

QUESTION : 6 (DES)

Find the average complexity of an exhaustive search against 2-key 3 DES.

QUESTION : 7 (DES)

Show that: $3DES_{\overline{k_1} \overline{k_2}}(\overline{P}) = \overline{3DES_{k_1 k_2}(P)}$