

1] Consider the joint random variables  $X$  and  $Y$  whose probability distribution is shown below:

		Y			
		A	B	C	D
X	A	0	$\frac{1}{8}$	$\frac{1}{4}$	0
	B	$\frac{1}{8}$	0	0	$\frac{1}{2}$

- a) Compute all of the marginal probabilities.
- b) Compute  $H(X, Y)$ .
- c) Compute  $H(Y)$ .
- d) Compute  $H(X | Y)$ .

2] Let  $n$  be a positive number,  $x_0, x_1, x_2 \dots, x_{n-1}$  be  $n$  distinct strings,  $X$  and  $Y$  be (not necessarily uniformly) random plaintext and ciphertext variables over

$$D_X = D_Y = \{x_0, x_1, x_2 \dots, x_{n-1}\},$$

and  $Z$  be a uniformly random secret key variable over

$$D_Z = \{0, 1, 2 \dots, n - 1\}.$$

Consider a secret-key cryptosystem in which encryption  $E: D_X \times D_Z \rightarrow D_Y$  and decryption  $D: D_Y \times D_Z \rightarrow D_X$  are defined by

$$\begin{aligned} E(x_i, z) &= x_{(i+z) \bmod n}, \\ D(x_i, z) &= x_{(i-z) \bmod n}. \end{aligned}$$

Prove that this secret-key cryptosystem gives perfect secrecy.

3] In each of the following, give the vector representation of the projection  $\pi$  such that

- a)  $\pi(\text{SHRINKAGE}) = \text{GARAGE}$
- b)  $\pi(\text{PRISM}) = \text{MISSISSIPPI}$
- c)  $\pi^{-1}(\text{HIPETRADO}) = \text{APHRODITE}$

4 Let  $a(x), b(x) \in GF(2^4)$  be defined by

$$\begin{aligned}a(x) &= x^3 + x^2 + 1, \\b(x) &= x + 1.\end{aligned}$$

a) Compute  $a(x) \oplus b(x)$ .

b) Compute  $a(x) \odot b(x)$  (modulo the prime polynomial  $m(x) = x^4 + x^3 + x^2 + x + 1$ ).

5 Complete an implementation of the AES *shiftRows* transformation. Assume the parameter  $s$  and return value are 2-dimensional AES state matrices whose first index is the row index and second index is the column index:

```
private byte[][] shiftRows(byte[][] s) {  
  
}
```

6 Consider the cipher block chaining (CBC) mode of AES operation. Let  $Z$  be the secret key block,  $X_1, X_2, X_3, \dots$  be the plaintext blocks encrypted by the sender,  $Y_1, Y_2, Y_3, \dots$  be the ciphertext blocks sent, and  $X'_1, X'_2, X'_3, \dots$  be the blocks recovered by the receiver.

a) Express the ciphertext block  $Y_i$  as a function of  $X_i, Y_{i-1}$ , and  $Z$ .

b) Express the recovered block  $X'_i$  as a function of  $Y_i, Y_{i-1}$ , and  $Z$ .

c) Prove  $X'_i = X_i$ .