PES UNIVERSITY

# PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

**UE18CS314**

## OCTOBER 2020: IN SEMESTER ASSESSMENT B Tech 5 SEMESTER
## TEST – 1
## UE18CS314 (4 credit) – APPLIED CRYPTOGRAPHY

| Time: 2 Hrs | Answer All Questions | Max Marks: 60 |
|---|---|---|

| | | | |
|---|---|---|---|
| 1. | a | For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case<br>The message space is M = {0, 1, 2, 3, 4} Algorithm Gen choses a uniform key from the key space {0, 1, 2, 3, 4, 5} Enck (m) returns [k + m mod 5] and Deck (c) returns [c-k mod 5]. | 5 |
| | b | The message space is M = {m ∈ {0,1}^t \| the last bit of m is 0}. Gen chooses a uniform key from {0,1} ^ t-1. $Enc_k$ (m) returns cipher-text: m ⊕ (k\|\|0), and $Dec_k$ (c) returns c ⊕ (k\|\|0). Note: \|\| represents concatenation | 5 |
| 2. | a | Alice needs to send the message "Enemy attacks tonight" to Bob. Use double columnar transposition cipher to find ciphertext with keys = {Crypt, Perfect}. | 4 |
| | b | Define Pseudo Random Permutation with example. | 3 |
| | c | Explain the working of one-time pad. | 3 |
| 3. | a | Why Permutation, Substitution used in DES encryption Algorithm? | 4 |
| | b | Given the s-box for s0 find the output for 011010 | 2 |
| | c | Explain the working of triple-DES. | 4 |
| 4. | a | Explain key expansion algorithm of AES for key "BEST CRYPTOGRAPHY" for first set of key word [w5-w8] with rcon given by. | 5 |

S[0]

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

Values of $rc_i$ in hexadecimal

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $rc_i$ | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1B | 36 |

| | | | |
|---|---|---|---|
| 4. | b) | Rajesh has designed a logistic regression classifier to predict the likelihood of stars being visible in the night sky based on the humidity reported on any day:<br><br>logit (p) = **log(p/(1-p)) = $\beta_0$ + $\beta_1$*humidity**, where p is the probability stars are visible at night.<br><br>Given that $\beta_0$ = 1.8185 and $\beta_1$ = -0.0665, answer the following questions:<br>(i) What does the value of $\beta_0$ mean?<br>(ii) If humidity on a day = 25, what is the probability with which stars are visible in the night sky according to this model? | 3 (1+2) |
| | c) | In a collection of 1000 small rocks collected on a river bed, 100 happen to be precious stones. All the 100 precious stones along with 100 other rocks have been classified as 'precious stones' by a logistic regression model. Write the entries of the confusion matrix for this classifier, clearly labeling the rows and columns. What further steps should be taken to plot the receiver operator characteristics (RoC) for this logistic regression model? | 3 (2+1) |
| 5. | a) | With a schematic sketch, briefly describe the key characteristics of the level, trend and seasonality components of an additive time series data. What are cyclic components and, why are they usually not accounted for in models for time series data? | 4 (3+1) |
| | b) | For the data given below, use MAPE to compare the forecast accuracy of single exponential smoothing (SES) with alpha = 0.7 with the forecast accuracy of the simple moving average (SMA) with a window size = 3 for time points t=5,6,7. [You can use the values of y that are available to make the forecasts for SMA and for SES assume the forecast, $F_4=y_4$.] | 3 |
| | c) | Suggest an application for each of the following techniques to model time series data<br>(i) Croston's method<br>(ii) Holt-Winter's method<br>(iii) ARIMA | 3 |
| 6 | a) | Write the equation corresponding to the two models given below (explain the symbols clearly):<br>(i) ARIMA(0,1,0)<br>(ii) ARIMA(1,0,1) | 4 (2+2) |
| | b) | Which model is better and why? (3+3) | 6 (3*2) |

| T | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $y_t$ | 10 | 11 | 12 | 16 | 17 | 19 | 20 |

| | Statistic | Model A | Model B | Better: Model A or Model B? | Why? |
|---|---|---|---|---|---|
| 1 | AIC | 258.24 | 251.42 | | |
| 2 | $R^2$ | 0.98 | 0.91 | | |
| 3 | RMSE | 0.048 | 0.051 | | |