





Security Package 2010/2011

| Serial | Algorithm | Input | | Marks |
|--------|---|---|---|-------|
| | | Plaintext | Key | |
| 1 | General Ceaser. | Text | integer | 2 |
| 2 | Monoalphabetic. | Text | Text | 2 |
| 3 | Autokey vigenere. | Text | Text | 2 |
| 4 | Repeating key Vigenere. | Text | Text | 2 |
| 5 | PlayFair. | Text | Text | 3 |
| 6 | Hill Cipher. | Text OR Numbers | Text OR Numbers  2X2 OR 3X3 | 4 |
| 7 | Rail Fence of depth Level n. | Text | Integer (n) | 4 |
| 8 | Columnar | Text | Integers | 4 |
| 9 | DES. | Text OR HEX | Text OR HEX | 5 |
| 10 | Multiplicative Inverse using Extended Euclid's. |  Integers (No., Base) | | 2 |
| 11 | AES. | Text OR HEX | Text OR HEX | 5 |
| 12 | RC4. | Text OR HEX | Text OR HEX | 4 |
| 13 | 3-DES. | Text OR HEX | Text OR HEX | 4 |
| 14 | RSA. | Integers (p, q, M, e) | | 5 |
| 15 | Diffie-Hellman key exchange. |  Integers (q, a, Xa, Xb) | | 3 |
| 16 | Elliptic curve cryptography (Key Exchange – Enc. /Dec.) |  Integers (q, a, b, k, na, nb) Points (G, Pm) | | 6 |
| 17 | Oral | | | 3 |
| 18 | Total | | | 60 |

Prof.Dr. Mohamed Hashem

T.A. (Eslam Gamal - Mohamed Saber – Heba Essam – Yara Medhat)

BONUS

| Serial | Item | Notes | Marks |
|--------|--|--|-------|
| 1 | Inverse Matrix Calculation in Hill cipher | If you calculate inverse matrix by code. | 3 |
| 2 | Multiplicative Inverse Using Extended Euclid's with polynomial | | 3 |
| 3 | SHA-1 | | 4 |
| 4 | Digital Signature | | 4 |
| 5 | Application | File Enc./Dec. (1) Image Enc./Dec (2) Audio Enc./Dec (2) Video Enc./Dec (2) | 7 |
| 6 | Code Style | OOP Design – Code Documentation | 3 |
| 7 | Interface | | 3 |
| 8 | Total | | 27 |

Notes:-

- 1- Bonus total = 20 Marks.
- 2- Max. Allowed bonus to group is (10) marks.
- 3- The other (10) marks will be used in ranking top (5) packages.
- 4- In application input (file – image – video – audio) then encrypt and decrypt it.

For examples:-

- 1- If group got (40/60) in package and in bonus (15/20) then total mark for this group will be (40 + 10 = 50/60).
- 2- If group got (60/60) in package and in bonus (20/20) then total mark for this group will be (60 + No Bonus = 60/60). The extra marks will be used in top (5) ranking.

Prof.Dr. Mohamed Hashem

T.A. (Eslam Gamal - Mohamed Saber – Heba Essam – Yara Medhat)