



**AF-1748**  
**M. Sc. (IT) (Sem. VIII) Examination**  
**April/May - 2015**  
**Information Security & Applications**  
**(New & Old)**

Time : 3 Hours]

[Total Marks : 70

**Instruction :**

<p>नीचे दृष्टावेक निशानीवाणी विगतो उत्तरवही पर अवश्य कपवी. Fillup strictly the details of signs on your answer book.</p> <p>Name of the Examination :</p> <p>☛ <b>M. Sc. (IT) (Sem. VIII)</b></p> <p>Name of the Subject :</p> <p>☛ <b>Information Security &amp; Applications (New &amp; Old)</b></p> <p>☛ Subject Code No. : <b>1 7 4 8</b> ☛ Section No. (1, 2,...): <b>Nil</b></p>	<p>Seat No. :</p> <table border="1" style="width: 100%; height: 20px;"><tr><td style="width: 15%;"></td><td style="width: 15%;"></td><td style="width: 15%;"></td><td style="width: 15%;"></td><td style="width: 15%;"></td><td style="width: 15%;"></td></tr></table> <div style="border: 1px solid black; border-radius: 15px; height: 60px; margin-top: 10px; display: flex; align-items: center; justify-content: center; padding: 10px;">Student's Signature</div>						

**Question 1: Answer following questions: (Any three)**

**[18]**

- (1) Explain different block cipher modes of operation with their advantages and limitations.
- (2) Explain DSS.
- (3) Explain different ways of distributing of public keys.
- (4) Explain various services of firewall.

**Question 2: Answer following questions:( Any Three)**

**[18]**

- (1) Explain Nidham Shroder protocol. What are the its limitations.
- (2) What is AH? Explain in tunnel and transport mode.
- (3) Write a note on PGP.
- (4) Define following:
  - (a) avalanche effect
  - (b) Non repudiation
  - (c) Authentication

**Question 3: Answer following questions: (Any Three)**

**[18]**

- (1) What is biometric? Explain any two biometric system with its advantages and limitations.
- (2) Explain any one public key algorithm with example.
- (3) Explain RC4 algorithm in detail.
- (4) Explain key generation algorithm of DES.

**Question 4: Answer following questions: (Any two)**

**[16]**

- (1) Explain Kerberos in detail.
- (2) Explain AES in detail.
- (3) Explain any one security protocol at transport layer.