Solution Info. Sec IT 7th
(061705)

Ans 1 (a) Time-of-check-to-time-of-use

(b) Incomple Mediation is a type of S/w flaw. Numerous buffer overflow in the linux Kernel, and most of these are due to incomplete medium.

(c) A Keylogger is a technology that tracks and record Consecutive key strokes on a keyboard.
It's a part of malware, spyware or an external virus.

(d) Anti-phishing tool.

(e) In cryptography, the encrypted message could be seen by anyone but it makes the message not understandable.
Steganography is hiding the message in another medium so that no body will notice the message.

Ans 2=) $P=5,\ q=7,\ n=pq=35$

$\phi(n)=(p-1)(q-1)=24$

$\therefore ed=1 \bmod \phi(n) \Rightarrow 5\cdot e=1 \bmod 24 \Rightarrow e=5$

Now

for f, $C=(m)^e \bmod n \Rightarrow C=(6)^5 \bmod 35 = 6 = f$

for e, $C=(5)^5 \bmod 35 = 10 = J$

for d, $C=(4)^5 \bmod 35 = 9 = i$

for c, $C=(3)^5 \bmod 35 = 33 = g$

for b, $C=(2)^5 \bmod 35 = 32 = 6 = f$

for a, $C=(1)^5 \bmod 32 = 1 = a$

$\therefore$ (fJigfa)

Ans 3 :) $q = 13$, $\alpha = 7$

$x_A = 3$, $y_A = 9$

$x_B = 8$, $y_B = 6$

Now

Secret key of A,

$$k = (y_B)^{x_A} \bmod q$$
$$= (6)^3 \bmod 13$$
$$= 216 \bmod 13 = 8$$

Secret key of user B,

$$k = (y_A)^{x_B} \bmod q$$
$$= (9)^8 \bmod 13$$
$$= 43046721 \bmod 13$$
$$= 3$$

∴ Secret key's are not same.

∴ Attack can't be possible.

Ans 4 : Virus: It's a self replicating program which is capable of copying itself and typically has detrimental effect such as corrupting the syst, or destroying data.

Trojan horse :) It's a prog. designated to breach the security of a computer syst. while ostensibly performing some innocuous function

Logic bomb :) It's a set of instructions secretly incorporated into a prog. so that if a particular condition is satisfied they will carried out, usually with harmful effects.

Ans 5 (a) :- * DES (Data encryption Standard)

* It's an algo. for encrypting and decrypting unclassified data.
* Uses Symmetric key Mechanism.
* It's a block cipher that takes PT String as I/P and created a C.T String of the same length
* Ⓐ Block size 64 bits.
  Ⓐ Key size 64 bits (56 + 8) bits
  8 bits for error dection.
  Ⓐ 16 rounds of operation.

(b) C = KP Mod 26

Me et me → UK it UK

(c) Cryptographic technique :-

(a) Substitution Cipher
(b) Transposition Cipher

Substitution Cipher → Ceaser Cipher
Monoalphabatic Cipher
Play-fair Cipher
Hill - Cipher.