

ID 2018963

Exam for Security and Networks [06-30195]

After inserting your student ID and the module name in the title, header and footer, write your answers between here and the statement of good academic conduct. Your ID and the module name will automatically appear on any subsequent pages.

Question1

A

1) $tA = g^{rA} \bmod p$

$\Rightarrow tx = 7^4 \bmod 11$

$\Rightarrow 3$

2) $(g^{rB} \bmod p, M * t^{rB} A \bmod p)$

$\Rightarrow (7^3 \bmod 11, 4X3^3 \bmod 11)$

$\Rightarrow (2,9)$

B

- i). I think it's a good key. Since the keys are all fresh, so it has the key freshness. And both the client and the server is using the key, so it has the key exclusivity. Then it's a good key
- ii). Yes. The AES generates keys, and with Authenticated Encryption, we can form a valid ciphertext if we know the key. And then send Encryption and hash function to ciphertext and MAC.

Question 2

a). The avoid traversal path attack.

b). I think Bob can do it. They have different user identifiers. Alice is the ruid for her directory. And Bob becomes euid after he logged into that host.

Question 3

a)

i). We can only use VPN to connect other networks, and VPN is secured with certificates and encryption with TLS, not decryption.

ii). Onion Routing.

b). I think it's possible.

The attacker acts as a man-in-the-middle:

1. $A \rightarrow C : E_{pk}(C) (N_a), A$
 - 1) $C(A) \rightarrow B = E_{pk}(B) (N_a), A$
 - 2) $B \rightarrow C(A) = E_{pk}(A) (N_a, N_b, B)$
2. $C \rightarrow A : E_{pk}(a) (N_a, N_b, B)$
3. $A \rightarrow C : E_{pk}(C) (N_b)$
 - 1) $C(A) \rightarrow B = E_{pk}(B) (N_b)$
4. $A \rightarrow C : \{M\} \# (N_a, N_c)$
 - 1) $C(A) \rightarrow B : \{M\} \# (N_c, N_b)$

Do not write below this line

Statement of good academic conduct

By submitting this assignment, I understand that I am agreeing to the following statement of good academic conduct:

- I confirm that this assignment is **my own work** and I have not worked with others in preparing this assignment.
- I confirm this assignment was written by me and is in my own words, except for any materials from published or other sources which are clearly indicated and acknowledged as such by appropriate referencing.
- I confirm that this work is not copied from any other person's work (published or unpublished), web site, book or other source, and has not previously been submitted for assessment either at the University of Birmingham or elsewhere.
- I confirm that I have not asked, or paid, others to prepare any part of this work for me.
- I confirm that I have read and understood the University regulations on plagiarism (<https://intranet.birmingham.ac.uk/as/registry/policy/conduct/plagiarism/index.aspx>).