Answer for 2nd Quiz.

Q1 θ function steps:

1. for all (x, z) such that $0 \leq x < 5$ and $0 \leq z < \overset{\approx 64}{w}$, let

$$C[x,z] = A[x,0,z] \oplus A[x,1,z] \oplus A[x,2,z] \oplus A[x,3,z] \oplus A[x,4,z]$$

2. for all (x, z) such that $0 \leq x < 5$ and $0 \leq z < w$, let

$$D[x,z] = C[(x-1) \bmod 5, z] \oplus C[(x+1) \bmod 5, (z-1) \bmod w]$$

3. for all triples (x,y,z) such that $0 \leq x < 5$, $0 \leq y < 5$, $0 \leq z < w$, let

$$A'[x,y,z] = A[x,y,z] \oplus D[x,z]$$

Another Representation

1. for all x such that $0 \leq x < 5$

$$C[x] = L[x,0] \oplus L[x,1] \oplus L[x,2] \oplus L[x,3] \oplus L[x,4]$$

2. for all (x, y) such that $0 \leq x < 5$, $0 \leq y < 5$

$$L'[x,y] = L[x,y] \oplus C[(x-1) \bmod 5] \oplus ROT(C[(x+1) \bmod 5], 1)$$

where $ROT(\underline{C}, 1)$ means rotate the C array by 1 bit,

In brief, the effect of θ is to XOR each bit in the state with the parities of two columns in the array. In particular, for the bit $A[x_0, y_0, z_0]$, the x-coordinate of one of the columns. is $(x_0-1) \bmod 5$, with the same z-coordinate, z_0, while the x-coordinate of the other column is $(x_0+1) \bmod 5$ with z-coordinate $(z_0-1) \bmod w$.

2 marks

So, if any change occurs in $L[0,0]$, in one round, the θ function can diffuse it to the lanes in columns 1 and 4, only. But it cannot diffuse the update to all lanes in one round. It requires one more round to diffuse the update in column 2 and 3 and 0 also.

3 marks

Q. 2

(A) Main Services

→ Confidentiality : The handshake protocol defines a shared secret key that is used for conventional encryption of ~~TS~~ TLS payloads. The allowed encryption schemes are AES, 3DES, RC4.

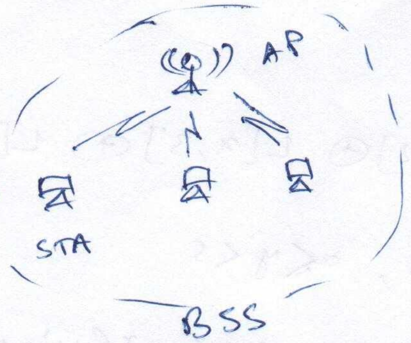
1

→ Message Integrity : The handshake protocol also defines a shared secret key that is used ~~for~~ to form Message Authentication code (MAC). TLS uses HMAC scheme in which MD5 or SHA-1 hash function is used.

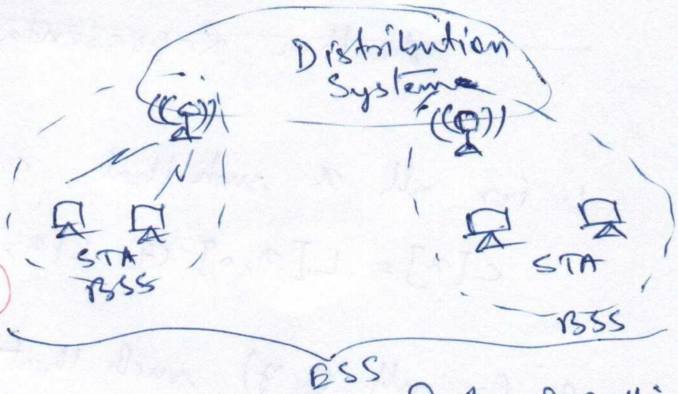
1

(B)

1

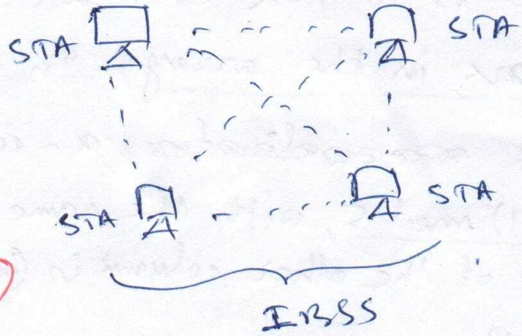


1



In this, STA to AP communications are ~~[illegible]~~ secured by 802.11i.
↑
BSS and ESS

But, End-to-End Security is pro~~b~~vided by upper layer protocols.



1

In IBSS, the communications beteen STA to STA are not secured by 802.11i.