1: What are digital certificates used for and who issues them?

Solution: Digital certificates are used to securely bind a public key owner with his/her public key and to distribute public keys to interested parties. Certificates are signed and issued by Certification Authorities (CA), trusted entities that verify the identity of public key owners and vouch for the trustworthiness of certificates.

2: What is a digital signature and what are its main properties?

3 Two bytes are known to have been encrypted by the same 8-bit RC4 stream producing C1 = 1111 0011 and C2 = 1111 1001 respectively. The bytes are believed to be non-capitalised vowels 'a':61(Hex) 'e':65, 'i':69, 'o':6F 'u':75. What are they? What is the 8 bit key?

Solution: C1 xor C2 = 0000 1010

Which combination of two vowels will produce 0000 1010 ? Think!!

'a' 0110 0001

'e' 0110 0101

'i' 0110 1001

'o' 0110 1111

'u' 0111 0101

Cannot be 'u' & another & can't be same letter, or we'd get '0000 0000' .

Over to you; (answer is what a donkey says).

(Don't forget, they can be in either order.)

4. Why is WEP not considered as a good security solution for WLANs and what are the main improvements of more recent standards (namely 802.11X and 802.11i)?

5. estimate the amount of time it would take to crack a DES encryption by testing all possibilities? If you have a 1GHZ processor, could you estimate the amount of time it would take to crack a DES encryption by testing all 2^56 possibilities?

Assuming:

2^56 keys

200 cycles to go through each iteration

1 Ghz Machine

(2^56) * 100/60/60/24/365/1000000000 = 228.49yrs