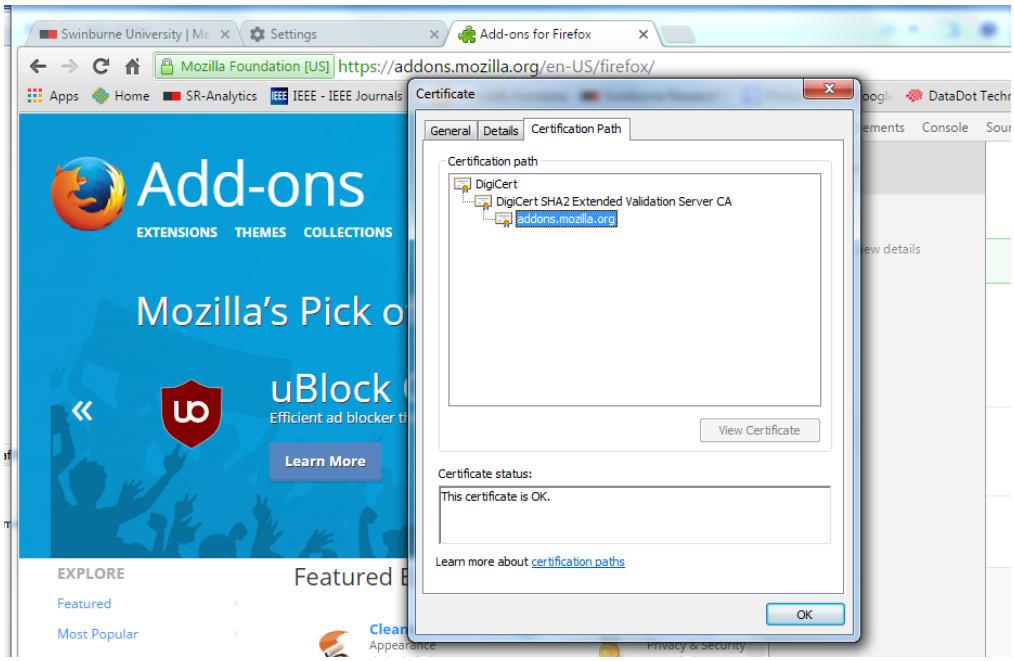
Tutorial Week 11

Questions

1. When purchasing goods via a website, why does the SSL/TLS protocol require the website to provide a digital certificate but not the person doing the purchasing?

2. The following is a digital certificate for addons.mozilla.org. The certificate has been verified by clicking the lock icon. What steps will have taken place in verifying the certificate?



3. Alice wishes to send a message to Bob. In order to guarantee the validity of identity, who will require a digital certificate in the following situations?

   a) The message is to be encrypted.

   b) The message is to be signed.

4. Test whether the following numbers are prime to a confidence level of 0.75.

   9, 11,

5. Test whether 5 is prime to a confidence level of 0.875

6. Consider the following simplified block encryption scheme:

   Plaintext is encrypted a byte at a time using the following steps:

   Step 1. The plain text is expanded to 12 bits by duplicating the first and last two bits (ie, abcdefgh becomes aabbcdefgghh

   Step 2. A 12 bit sub key is XORed with the expanded text from step 1

   Step 3. The bit sequence from step 2 is split into two 6 bit sequences and fed into the following two S-BOXes

Tutorial Week 11

Step 4. The output of the S-BOXes is concatenated and fed through a permutation process that reverses the bit sequence order

What is the output for a plaintext input of 1001 0100 and a 12 bit sub-key of 1001 0011 1010?

S1		**Middle four bits**															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110
	01	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000
	10	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000
	11	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101

S2		**Middle four bits**															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110
	01	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000
	10	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000
	11	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101