2020/21 - Midterm 2, 22 Dec 2020 – open questions

Q1: (TLS Padding Oracle Attack) – Assume a CBC-based block encryption scheme which uses block sizes of 4 bytes each. Assume that the attacker sees the following ciphertext comprising 6 blocks (hex notation):

f1 aa 11 04 || 34 35 f1 20 || 07 07 07 07 || 73 73 73 73 || 65 61 fb 08 || 91 11 5f 10

Assume now that the server is vulnerable to a Padding Oracle attack, and assume that the fourth block (the one underlined) contains a secret code which is either 01 01 01 01 or 02 02 02 02. Which Chosen ciphertext message should the attacker send to the server/oracle to as to determine the code? *[students MUST explain why and how they obtained the answer, otherwise the answer, even if correct, will not be considered valid]*

Q2: (block cipher modes) – Assume a toy block cipher based on 4 bit blocks. The block cipher uses a key which implements the permutation illustrated in the table below.

0) show the construction of both the CBC mode and the CTR mode

1) Using CBC, decrypt the ciphertext CT = (1101) 1001 0101 0110

2) using CTR, encrypt the plaintext PT = 0001 0010 0011 using as Initial counter, the value 1100

input	**output**
0000	0001
0001	0010
0010	1011
0011	1111
0100	1101
0101	0000
0110	0011
0111	1001
1000	0110
1001	1000
1010	0101
1011	0111
1100	1110
1101	1100
1110	1010
1111	0100

Q3: (RSA) – A toy RSA scheme uses modulus N=143 and public key e=103.

1. After having found Phi[N], find the decryption key d by using the Extended Euclidean Algorithm;
2. decrypt the ciphertext CT=11 by using the square and multiply algorithm

[students MUST step-by-step show the application of either the Extended Euclidean Algorithm for answer 1, as well as the Square an Multiply algorithm for answer 2, otherwise the answer, even if correct, will not be considered valid]