2021/22 - Midterm 2, 21 De c 2021 – open questions

Q1: (block cipher modes) – Assume a toy block cipher based on 4 bit blocks. When using key A, the block cipher implements the permutation show on the left (black table), whereas with key B, the permutation is shown on the right (red table).

0) show the construction for both CBC and CTR modes;
1) Using CBC, key A, and IV=1010, encrypt the ciphertext CT = 1000 1000 1000
2) using CTR and key A, decrypt CT = 0111 0001 1000 using as Initial counter the value 1100
3) Is the permutation produced with one of these two keys preferable than the other, or are these two permutations equivalent? MOTIVATE THE ANSWER.

Key A

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

Key B

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

Q2: (RSA) – A toy RSA scheme uses two primes p=11 and q=23, and modulus N=253. Assuming that the public key is e=7, compute the private key d by step-by-step using the Extended Euclidean Algorithm *[the answer, even if correct, without the Extented GCD steps will not be considered valid]*

Q3: (PKCSv1.5) – Describe the PKCSv1.5 RSA padding, and discuss under which conditions such scheme may yield a Bleichenbacher Oracle.

Q4: (BEAST attack) – An attacker sees the following ciphertext, encrypted with CBC and with IV=1234:

(1234) | A1B2 | C3D4 | E5F6

The attacker knows that a secret code hidden in the above second block (i.e. the one encrypted as C3D4) is either 1111 or 2222. The attacker can now perform a CPA, and **can predict that the next IV will be 5678**.

Which chosen plaintext you would submit to decrypt the above secret code, and why?