

open questions

Q1: (RSA)

- 1) Apart from the toy sizes, among the following RSA modules which one you would prefer, and why? $N_1 = 11 \times 23$, $N_2 = 17 \times 19$;
- 2) Assuming now to select the RSA system using modulus $N = 11 \times 23$ and $e=3$, compute the private key d
- 3) encrypt message $m=127$
- 4) Starting from the previous ciphertext, show which ciphertext value you would submit to a Bleichenbacher-type oracle which discloses the first bit of the plaintext, to verify that the encrypted message is greater than 63.

[Compute all answers showing calculations using either the Extended GCD steps and the Square and multiply algorithms]

Q2: (AES-GCM) – Show an approximate schematic of the AES-GCM construction (or at least explain what are the key aspects of such cipher), and briefly discuss what happens if the IV is reused.

Q3: (BEAST attack) – toy block size = 4 bit - An attacker sees the following ciphertext, encrypted with CBC and IV=0110:

(0110) | 0111 | 1100 | 0101 | 0100 | 1110

The attacker wants to check whether a secret code hidden in the underlined block is the value 1000. The attacker can now perform a CPA, and **can predict that the next IV will be 0111**. Which chosen plaintext you would submit to decrypt the above secret code, and why?