Cryptology, homework sheet 4

Due 12 October 2021, 13:15

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.

1. The lectures showed how TEA can be used to encrypt some input block b. Explain how decryption works, i.e., how to compute the input given the output and the key.
   Hint: Show how to invert one round and how to compose these steps.
   Hint: Looking at the diagram in lecture V can help.

   4 points

2. The proper definition of Wegman–Carter MAC puts

$$t_i = \left(\sum_{j=1}^{k} c_{i,j} r^{k+1-j} \bmod p \right) + s_i \bmod 2^n$$

   for c_i a ciphertext of kn bits and $p > 2^n$ a prime.

   Show that it is important that the powers of r start at r^1 rather than at r^0, i.e., show how an outside attacker who does not have access to r or any of the s_i but sees some (c_i, t_i, i) can compute some valid (c', t', i) on a new ciphertext $c' \neq c_i$ if instead the definition is

$$t' = \left(\sum_{j=1}^{k} c_j r^{k-j} \bmod p \right) + s_i \bmod 2^n.$$

   6 points