Cryptology, homework sheet 7

Due 20 October 2021, 10:30

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.
For this sheet you can use Sage for exponentiations modulo large numbers and gcds. Make sure to document what you type and what the answers are.

1. 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

2. Bob uses public key $(n, e) = (396553, 17)$. His secret key is a CRT key using $p = 541$ and $q = 733$.

   (a) Compute the full secret key (n, p, q, d_p, d_q, u). 1.5 points

   (b) Decrypt ciphertext $c = 234040$ using the CRT method and verify your result by reencrypting it.
   Make sure to document your computation, i.e., state the values for $c_p, m_p, \ldots$
   Note that there was a typo on the slides in the YouTube video for computing m; the slides have been fixed. 2.5 points

3. This exercise is about factoring.

   (a) Use the $p - 1$ method to factor $n = 396553$ with basis $a = 8$ and exponent $s = \mathrm{lcm}(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$. Make sure to state the value for s and the result of the exponentiation modulo n. Determine both factors of n. 2 points

   (b) The factorization of 540 is $540 = 2^2 \cdot 3^3 \cdot 5$ and that of 732 is $732 = 2^2 \cdot 3 \cdot 61$. Explain why the factorization in (a) was successful.
   Hint: Check whether $a = 2$ would have worked.

   3 points