Cryptology, homework sheet 5

Due 10 October 2023, 13:30

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 exercise you can use Sage for computations modulo p, q and n, including exponentiations. You may not use the built-in function for solving the DLP but follow the algorithm specified. Make sure to document what you type and what the answers are.

1. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for some prime p. Let $p = 1249$ and note that $p - 1 = 2^5 \cdot 3 \cdot 13$. A generator of $\mathbb{F}_p^*$ is $g = 7$. Bob's public key is $h_b = g^b = 1195$.

   Use the Pohlig-Hellman attack to compute Bob's secret key b; make sure to handle each power of 2 separately as in the algorithm description.

   Verify your answer, i.e., compute g^b. | 10 points |

2. For RSA 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) Perform one round of the Fermat test with base $a = 2$ to test whether p is prime. | 0.5 points |

   (c) 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 $c_p, m_p, \ldots$ | 3 points |