Modern Cryptography Dec 17, 2019

Homework 11

Lecturer: Daniel Slamanig, TA: Karen Klein, Guillermo Perez Due: 23.59 CET, Jan 8, 2020

To get credit for this homework it must be submitted no later than Wednesday, December 11th via TUWEL. If you have not registered for the tutorial (192.063 Tutorial on Introduction to Modern Cryptography 2019W) on TUWEL, please do so. If you are unable to register for the course on TUWEL for some reason, submit your homework via email to via email to `michael.walter@ist.ac.at`, please use "MC19 Homework 11" as subject.

1. Textbook RSA Encryption

   - Prove the correctness of the textbook RSA encryption algorithm as introduced in the lecture, i.e., show that for all $n \in \mathbb{N}$, $((N,d),(N,e)) \leftarrow \mathsf{KeyGen}(1^n)$ any $m \in \mathbb{Z}_N$ it holds that $(m^e)^d \equiv m \pmod{N}$.
   - **[11.20 in book, 2nd edition]** Fix an RSA public key (N,e) and assume we have an algorithm $\mathcal{A}$ that always correctly computes $\mathsf{lsb}(x)$ (i.e., the least significant bit of x) given $x^e \bmod N$. Write full pseudocode for an algorithm $\mathcal{A}'$ that computes x from $x^e \bmod N$.
   - A message m is encrypted using textbook RSA encryption with keys $(493,3)$ and $(493,5)$ yielding ciphertexts 293 and 421 respectively. Use the fact that the two public keys share the same modulus to recover m and describe how the attack works (Hint: common modulus attack).

2. Insecure Public-Key Encryption

   - Let us assume the following public-key encryption scheme. Chooses integers $a, b, a', b' \in \mathbb{N}$, with $a > 1$, $b > 1$, and compute:

     $$M = ab - 1, \quad e = a'M + a, \quad d = b'M + b, \quad n = \frac{ed - 1}{M}.$$

     The public key is (n,e), the private key is d. To encrypt a plaintext m, one computes $c = em \bmod n$. Alice decrypts a ciphertext c as $m = cd \bmod n$.

     – Verify that decryption recovers the message.

     – Show how the Euclidean algorithm can be efficiently used to break the encryption scheme.