

CSE 794 Homework 5

Due: Tuesday, March 10 by class time

Final exam: Wednesday, March 18, 11:30-1:18.

Open book/notes.

1. Fix the RSA modulus n , and assume there is an adversary A running in time t for which

$$\Pr\left[A(x^e \bmod N) = x : x \leftarrow_u Z_N^*\right] = 0.01.$$

That is, A can decrypt the ciphertext of a random message x with probability 0.01.

Construct an adversary A' for which

$$\Pr\left[A'(x^e \bmod N) = x : x \leftarrow_u Z_N^*\right] = 0.99.$$

The running time t' of A' must satisfy $t' \leq \text{poly}(t, \log N)$.

Hint: use the homomorphism property.

2. In a public-key system using RSA, you intercept a ciphertext $c = 60$ sent to a user whose public key is $n = 155$ and $e = 3$. What is the plaintext m ?
3. In an RSA system, the public key of a user is $e = 31$, $n = 3599$. What is the private key of this user?
4. Assume that Alice's RSA keys are (n_1, e_1, d_1) , and Bob's are (n_2, e_2, d_2) . Suppose Alice generates a signed and encrypted message by:

$$c := (m^{d_1} \bmod n_1)^{e_2} \bmod n_2.$$

That is, Alice first signs the message using her private key d_1 and then encrypts the signed message using Bob's public key e_2 . The message m is not sent along with the ciphertext.

Q: Can Bob always recover m correctly from c ? Justify your answer.