

BMEG3120: Exercise List 11

Problem 1. Calculate $50^{45} \bmod 1961$.

Problem 2. Consider an RSA cryptosystem with $p = 17$, $q = 13$ (hence, $n = pq = 221$), and $e = 35$.

- What is the value of d ?
- Let (e, n) be the public key of Alice. If we use it to encrypt a message $m = 78$, what is the ciphertext C ?
- Let (d, n) be the private key of Alice. If she receives a ciphertext $C = 65$, what is the original message m ?
- If you receive a message $m = 93$ from Alice and her digital signature 188, do you think that this message indeed comes from her?

Problem 3. Suppose that Alice's public key is $(13, 77)$. You are a hacker. Suppose that you have intercepted an encrypted message $C = 64$ for Alice. Now, break RSA by figuring out the original message.