BMEG3120: Exercise List 11

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

Answer. $50^2 \mod 1961 = 539$
$50^4 \mod 1961 = 539^2 \mod 1961 = 293$
$50^8 \mod 1961 = 293^2 \mod 1961 = 1526$
$50^{16} \mod 1961 = 1526^2 \mod 1961 = 969$
$50^{32} \mod 1961 = 969^2 \mod 1961 = 1603$

Therefore, $50^{45} \mod 1961 = 50^{32} \cdot 50^8 \cdot 50^4 \cdot 50 \mod 1961 = 1603 \cdot 1526 \cdot 293 \cdot 50 \mod 1961 = 1412$.

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?

Answer.

- $\phi = (p-1)(q-1) = 192$. d needs to satisfy the equation $35 \cdot d \mod 192 = 1$. Hence, $d = 11$.
- $C = m^e \mod n = 78^{35} \mod 221 = 65$.
- $m = C^d \mod n = 65^{11} \mod 221 = 78$.
- Let $C = 188$. $C^e \mod n = 188^{35} \mod 221 = 154$. Since this is different from m, we reject the message.

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.

Answer. We factor 77 into $p = 7$ and $q = 11$. Hence, we know that $e = 13$ and $d = 37$. Therefore, Alice's private key is $(37, 77)$. We can therefore restore the message $m = C^d \mod 77 = 64^{37} \mod 77 = 15$.