Crypto Homework 5

Noah Wong

October 2018

1.) Use the Euclidean algorithm to find the greatest common divider of 294,906 and 178,549. Also find integer multiples of these numbers who sum is the gcd.

$$\begin{aligned}
294,906 =&178,549(1) + 116,357\\
178,549 =&116,357(1) + 62192\\
116,357 =&62192(1) + 54165\\
62192 =&54165(1) + 8027\\
54165 =&8027(6) + 6003\\
8027 =&6003(1) + 2024\\
6003 =&2024(2) + 1955\\
2024 =&1955(1) + 69\\
1955 =&69(28) + 23\\
69 =&23(3)
\end{aligned}$$

Thus by the euclidean algorithm the gcd of 294,906 and 178,549 is 23. Finding the integer multiples of these numbers who sum is the gcd involves using the Euclidean algorithm above in reverse order.

$$\begin{aligned}
23 =&1955 - 69(28)\\
23 =&1955 - (2024 - 1955)(28)\\
23 =&1955(29) - 2024(28)\\
23 =&(6003 - 2024(2))(29) - 2024(28)\\
23 =&6003(29) - 2024(86)\\
23 =&6003(29) - (8027 - 6003)(86)\\
23 =&6003(115) - 8027(86)\\
23 =&(54165 - 8027(6))(115) - 8027(86)\\
23 =&54165(115) - 8027(776)\\
23 =&54165(115) - (62192 - 54165)(776)\\
23 =&54165(891) - 62192(776)\\
23 =&(116357 - 62192)(891) - 62192(776)\\
23 =&116357(891) - 62192(1667)\\
23 =&116357(891) - (178549 - 116357)(1667)\\
23 =&116357(2558) - 178549(1667)\\
23 =&(294906 - 178549)(2558) - 178549(1667)\\
23 =&294906(2558) - 178549(4225)
\end{aligned}$$

So the integers you multiple by are 2558 and -4225.

2.) Let $p = 19, q = 29$, and $e = 215$. Encipher the message $M = 15$ using the RSA scheme. Next, decipher your ciphertext to make sure you get 15 back.

We start by defining $N = pq = 19 * 29 = 551$, and find the cipher text of $M = 15$. We need to compute 15^{215} (mod 5)51. We can do this by fast exponentiation.

$$15^2 \equiv 225 \pmod{551}$$
$$15^4 \equiv 225^2 \equiv 484 \pmod{551}$$
$$15^8 \equiv 484^2 \equiv 81 \pmod{551}$$
$$15^{16} \equiv 81^2 \equiv 500 \pmod{551}$$
$$15^{32} \equiv 500^2 \equiv 397 \pmod{551}$$
$$15^{64} \equiv 397^2 \equiv 23 \pmod{551}$$
$$15^{128} \equiv 23^2 \equiv 529 \pmod{551}$$

Since $215 = 128 + 64 + 16 + 4 + 2 + 1$ we calculate $15^{215} \pmod{551}$ as,

$$\begin{aligned} 15^{215} \equiv& 15^{128+64+16+4+2+1} \pmod{551} \\ 15^{215} \equiv& 15^{128} * 15^{64} * 15^{16} * 15^4 * 15^2 * 15 \pmod{551} \\ 15^{215} \equiv& 529 * 23 * 500 * 484 * 225 * 15 \pmod{551} \\ 15^{215} \equiv& 280 \pmod{551} \end{aligned}$$

Thus the encrypted message is $c = 280$. Next we need to check if this is the correct. So we need to find the decryption element.Since $\phi(N) = (p-1)(q-1) = 18 * 28 = 504$, thus $ed \equiv 1 \pmod{504}$. We can find d by using the euclidean algorithm on 504 and 215.

$$\begin{aligned} 504 =& 215(2) + 74 \\ 215 =& 74(2) + 67 \\ 74 =& 67(1) + 7 \\ 67 =& 7(1) + 4 \\ 7 =& 4(1) + 3 \\ 4 =& 3(1) + 1 \end{aligned}$$

We can rewrite these equations as,

$$\begin{aligned} 74 =& 504 - 215(2) \\ 67 =& 215 - 74(2) \\ 7 =& 74 - 67(1) \\ 4 =& 67 - 7(9) \\ 3 =& 7 - 4(1) \\ 1 =& 4 - 3(1) \end{aligned}$$

Find the inverse of 215 as follows:

$$\begin{aligned}
1 =& 4 - (7 - 4)\\
1 =& 4(2) - 7\\
1 =& (67 - 7(9))(2) - 7\\
1 =& 67(2) - 7(19)\\
1 =& 67(2) - (74 - 67)(19)\\
1 =& 67(21) + 74(-19)\\
1 =& (215 - 74(2))(21) + 74(-19)\\
1 =& 215(21) + 74(-61)\\
1 =& 215(21) + (504 - 215(2))(-61)\\
1 =& 215(143) + 504(-61)
\end{aligned}$$

Thus $215 * 143 \equiv 1 \pmod{504}$ and $d = 143$. Checking to see if the message is correct we get,

$$280^{143} \equiv 15 \pmod{551}.$$

Thus the have correctly applied RSA to the message $M = 15$.

3.) Typically the primes multiplied together to form the modulus for RSA are of about the same size. Explain why this might be.

Factoring a number with two large primes is difficult, however it becomes easier if one of the primes is smaller. Using brute force to check for which primes factor a number N you only need to check if N is divisible by primes up to $\sqrt{N}$. Thus if you have $N = pq$ where p and q have a large difference between the two. The brute force method requires less work because you have less primes you have to check.

4.) Formulate a man-in-the-middle attack, similar to the attack described in Example 3.13 on page 126 for the RSA public key cryptosystem.

Using our normative terminology, to avoid confusion, of Alice, Bob and Eve representing two innocent souls Alice and Bob attempting to communicate with a devious Eve mucking up their plans. In this situation Eve is successfully able to intercept messages and impersonate both Alice and Bob. Alice and Bob are naively using RSA without MAC addresses to confirm their identities so Eve can use a 'man-in-the-middle' attack.

We start with Alice who chooses her RSA numbers, primes p_a and q_a which gives her $N_a = p_a q_a$ and an encryption exponent e_a such that $gcd(e_a, (p_a - 1)(q_a - 1)) = 1$. However before she is able to send out this information to the world Eve is able to block it and send out her own information in place of Alice's. Eve in the place of Alice sends out her own RSA encryption keys, primes p_e and q_e such that $N_e = p_e q_e$ and an encryption exponent e_e. Bob will receive Eve's RSA numbers thinking there are Alice's. Then whenever he wants to send a message to Alice he will take $m^{e_e} \pmod{N_e}$ and send it to Alice. Again Eve will be in the middle and since she knows q_e, p_e and e_e thus she also knows the decryption exponent d_e. So she will decrypt $m^{e_e^{d_e}} \equiv m \pmod{N_e}$ and discover the message Bob is attempting to send to Alice. Then to avoid suspicious she will encrypt this message with Alice's original key $m^{e_a} \pmod{N_a}$ and send it along to Alice. Then Alice will be able to decrypt this message normally and receive Bob's message. If Eve is able to pull this off successfully neither Bob or Alice will know that Eve can read all their messages. This makes this attack especially heinous, compared to attacks that can decode a single message. Next time Alice and Bob will learn to use MAC address or a more complex crypto-scheme.