COMP90043 Cryptography and Security
Semester 2, 2021, Workshop Week 6 Solutions

Revision:

1. Perform encryption and decryption using the RSA algorithm, as in Figure 9.5 (of the textbook), for the following:

   (a) p = 3; q = 11, e = 7; M = 5
   $n = 33; \phi(n) = 20; d = 3$
   $C = 5^7 \bmod 33 = 14$
   $M = 14^3 \bmod 33 = 5$

   (b) p = 5; q = 11, e = 3; M = 9
   $n = 55; \phi(n) = 40; d = 27$
   $C = 9^3 \bmod 55 = 14$
   $M = 14^{27} \bmod 55 = 9$

   (c) p = 7; q = 11, e = 17; M = 8
   $n = 77; \phi(n) = 60; d = 53$
   $C = 8^{17} \bmod 77 = 57$
   $M = 57^{53} \bmod 77 = 8$

   (d) p = 11; q = 13, e = 11; M = 7
   $n = 143; \phi(n) = 120; d = 11$
   $C = 7^{11} \bmod 143 = 106$
   $M = 106^{11} \bmod 143 = 7$

   (e) p = 17; q = 31, e = 7; M = 2
   $n = 527; \phi(n) = 480; d = 343$
   $C = 2^7 \bmod 527 = 128$
   $M = 128^{343} \bmod 527 = 2$

Questions:

1. State Fermat's and Euler's theorems. Using these two theorems simplify the following equations.

   Fermat's: if p is prime, then for any integer a,

   $$a^p = a \pmod p$$

   Euler's: if a and n are coprime, then

   $$a^{\phi(n)} = 1 \pmod n$$

   (a) $4^{12} \pmod{21} = 1 \pmod{21}$
   (b) $2^{22} (\bmod\ 23) = 1 \pmod{23}$
   (c) $3^{17} (\bmod\ 17) = 3 \pmod{17}$
   (d) $5^{35} (\bmod\ 17) = 5^3 \pmod{17} = 6 \pmod{17}$
   (e) $73^{10001} (\bmod\ 101) = 73 \pmod{101}$

2. Solve for x satisfying the following simultaneous congruences:

   $$x \equiv 7 \pmod{11},$$
   $$x \equiv 9 \pmod{13}.$$

   7 mod 11 is congruent to $18, 29, 40, 51, 62, 73, 84, 95, 106, 117, 128, 139$. 9 mod 13 is congruent to $22, 35, 48, 61, 74, 87, 100, 113, 126, 139$. Hence, $x = 139$.

   Let $a_1 = 7$ and $a_2 = 9$; $n_1 = 11$ and $n_2 = 13$. There exists m_1 and m_2 such that $m_1 n_1 + m_2 n_2 = 1$. Using Extended Euclidean algorithm, we find $m_1 = 6$ and $m_2 = -5$. Finally, $x = a_1 m_2 n_2 + a_2 m_1 n_1 = 7 \times -5 \times 13 + 9 \times 6 \times 11 = 139$.

3. Solve for x satisfying the following simultaneous congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5), \\ x &\equiv 2 \pmod 7. \end{aligned}$$

$x = -82 \pmod{105} = 23 \pmod{105}$

4. Assume that Alice chooses two primes 43 and 47 to construct her RSA key prime factors. Help her to set up public and private keys and demonstrate encryption and decryption with an example. Choose the smallest possible exponent for the public key.

$n = 2021; \phi(n) = 1932.$
Smallest (non-trivial) e is 5.
Therefore, $5 \times d = 1 \bmod 1932; d = 773.$

Suppose we have $M = 313.$
For encryption, $C = 313^5 \bmod 2021 = 464.$
For decryption, $M = 464^{773} \bmod 2021 = 313.$

6. $GCD(m, n)$ gives you either p or q.

7. Explain how you can use RSA encryption function to construct a digital signature scheme.

- Public Key: $< n, e >$
- Private Key: $< n, d >$
- Hash Function: $H(m)$
- Compute Signature $s = H(M)^d \bmod n$; $[M, s]$ form message signature pair.
- Verification Algorithm: If $H(M) == s^e \bmod n$ then accept the signature else declare verification failure.

8. With RSA, discuss how the concept of Blinding can be implemented?

RSA allows the incorporation of Blinding in two ways:

- By allowing the multiplication of the plaintext message with an arbitrary number before performing exponentiations which allows the operations to be performed not on the real input or the real output. Not all functions can use this approach. One example is when Alice wants Bob to return to her the result of a function F which only Bob has access to. But Alice doesn't want Bob to know the input M. By using blinding, Alice blinds, encrypts, and sends M' to Bob. Bob then calculates and returns the value of $F(M')$. Alice then decrypts $F(M')$ and reverses the blinding to get $F(M)$.
- RSA supports Blind Signatures, wherein similar to the above concept; the content of the passed message is oblivious to the person signing it. This is applicable when the authenticity of the message needs validation from an entity who did not write the message.