King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Department of Computer Engineering

ICS 555 – Data Security and Encryption (T162)

Homework # 03 (due date & time: Wednesday 10/05/2017 during class period)

Problem # 1 – 20 points: Given the RSA signature scheme with the public key ($N = 9797$, $e = 131$), which of the following signatures are valid?

1. ($M = 123$, sig(M) = 6292)
2. ($M = 4333$, sig(M) = 4768)

Problem # 2 – 20 points: The parameters of DSA are given by $p = 59$, $q = 29$, $g = 3$, and Bob's private key is $d = 23$:

1. Show the process of signing (Bob) and verification (Alice) for $h(M) = 17$ and $r = 25$.
2. If instead of Alice receiving $h(M) = 17$ she receives $h(M) = 15$, show that Alice detects that the signature is invalid.

Problem # 3 – 10 points: Find the number of collisions you would expect to find if a hash function generates an n-bit output and you hash m randomly selected messages.

Problem # 4 – 20 points: Consider a "2 out of 3" secret sharing scheme.

1. **(8 points)** Suppose that Alice's share of the secret S is (1, 0), Bob's share is (2, 2), and Charlie's share is (3, 4). **What is the secret *S*? What is the equation of the line?**
2. **(12 points)** Suppose that the arithmetic is taken modulo 13, that is, the equation of the line is of the form ($ax + by = c$) mod 13. Suppose that Alice's share of the secret S is (1, 7), Bob's share is (2, 3), and Charlie's share is (3, 12). **What is the secret *S*? What is the equation of the line, mod 13?**

Problem # 5 – 10 points: Consider the 1 out of 2 OT protocol presented in class. Suppose Alice's public key is ($N = 55$, $e = 7$), and Alice's private value $d = 23$. Also, suppose Alice has the messages $m_0 = 35$ and $m_1 = 12$. Assume that Alice sends $x_0 = 4$ and $x_1 = 40$ in the first message, and Bob is interested in obtaining m_0 and chooses $k = 30$. Show that Bob will successfully obtain m_0 but fails to successfully obtain m_1.

Problem # 6 – 20 points: Consider the Fiat-Shamir protocol presented in class. Suppose the public values are $N = 55$ and $v = 5$. Suppose Alice sends $x = 4$ in the first message, Bob sends $e = 1$ in the second message, and Alice sends $y = 30$ in the third message.

1. Show that Bob will verify Alice's response in this case.
2. Find Alice's secret, S.