Internet Infrastructure Security (COMP444)
A4

Due at 11:55pm on 12 March 2015
Submission site: `https://submit.comp.polyu.edu.hk/`

Rocky K. C. Chang

March 6, 2015

1. `[6 marks]` (The Chinese Remainder Theorem, CRT) Consider $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and $P = p_1 \times p_2 \times p_3 = 30$, and $x \in \{0, 1, 2, \cdots, 29\}$. We would like to compute $12^{9999}\ mod\ 30$. We know that by the CRT, $12^{9999}\ mod\ 30$ can be represented by $(0\ mod\ 2, 0\ mod\ 3, 12^{9999}\ mod\ 5)$.

   (a) `[4 marks]` What is the value of $12^{9999}\ mod\ 5$? (Hint: $12^4 \equiv 1\ (mod\ 5)$).

   (b) `[2 marks]` What is the value of $12^{9999}\ mod\ 30$? (Hint: solving the CRT by setting $P_3 = 6$ and $y_3 = 1$ in the formula on slide 25 of L5).

2. `[6 marks]` (Multiplicative inverses) Consider $Z_p = \{0, 1, \cdots, p-1\}$, where p is a composite number. You are given two numbers a and b from Z_p.

   (a) `[3 marks]` If a or b does not have multiplicative inverse, show that $c = a \times b \mod p$ also does not have multiplicative inverse.

   (b) `[3 marks]` If both a and b have multiplicative inverses, show that $c = a \times b \mod p$ also has multiplicative inverse.

3. `[6 marks]` ($e = 3$ for RSA) Answer the following questions concerning the choice of e for RSA. Hint: e must be co-prime with $(p-1)(q-1)$.

   (a) `[2 marks]` Why is 3 the smallest possible value for e?

   (b) Could $e = 3$ be possibly be used for the following values of p and q?

      i. `[2 marks]` $p \mod 3 = 1$ and $q \mod 3 = 1$.

      ii. `[2 marks]` $p \mod 3 = 2$ and $q \mod 3 = 2$.

4. `[6 marks]` (RSA signature) Alice wants Bob to sign a message m. Assume that Bob's signing is based on RSA. However, she does not want Bob to see the message. Therefore, Alice "blinds" the message by computing $m' = mk^e \mod n$, where k is a random value between 1 and n and $gcd(k, n) = 1$. Alice then presents m' to Bob for his signature. How will Alice obtain Bob's signature on m ($m^d \mod n$) from Bob's signature on m'? Hint: p. 9 of the RSA slides.