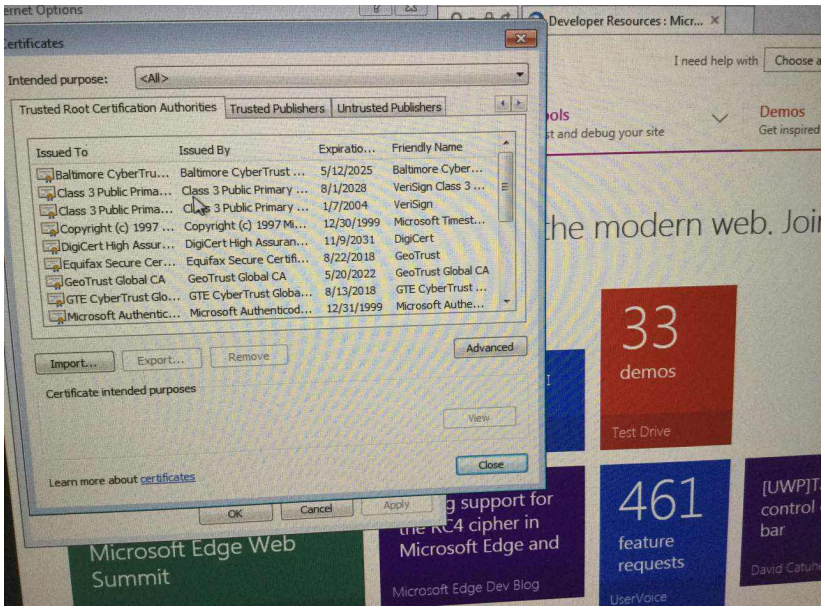
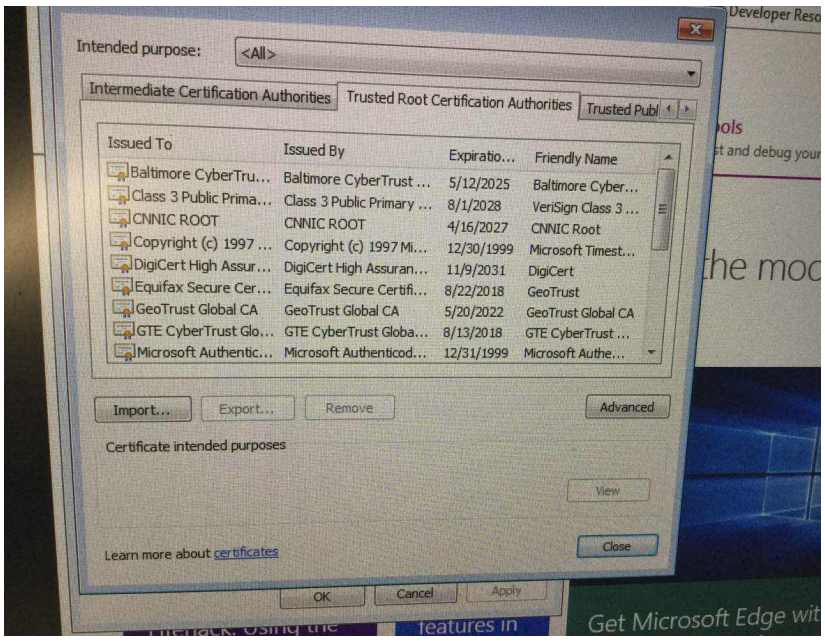
Zelong Li
24569650
Discussion 102
TA: Qi Zhong
CS161 Homework 1

1.
Before I visit the site, it does not appear in IE 11's signed certificates. However, after I go to https://cnnic.cn, CNNIC appears in its signed certificates. This implies that IE 11 put this website into its signed certificates without noticing me and it would trust certificates without checking the reliability. The security risk in using Internet Explorer 11 is that the certificates leaked described in the article would monitor my activities on my computer but IE 11 would not warn me.





2.
e = 11
n = 5352499
Since n = pq where p and q are large prime, after factorization:
n = pq = 1237 × 4327
p = 1237
q = 4327
(p-1)(q-1) = (1237-1)×(4327-1) = 5346936
$ed \equiv 1 \bmod (p-1)(q-1) \equiv 1 \bmod 5346936$
So, $d = 11^{-1} \bmod 4860851 = 4860851$
$m1 = 195125^{4860851} \bmod 5352499 = 4491763$
$m2 = 3886883^{4860851} \bmod 5352499 = 32$
$m3 = 4748558^{4860851} \bmod 5352499 = 23$

3.
This is not a good counter argument because in the case we can only get one square root in modulo n (n=pq), there is still a chance for us to factor n. In the case describe in the question, we can only get one square root of a square in modulo. However, if we have two squares in modulo n, we can one root of each square in modulo n and there is a chance that the greatest common divisor of the sum of these two square roots and n is p or q. Therefore, the counter argument is not a good one.
Example:
$\sqrt{1} = \{1, -1, 4, -4\} = \{1, 4, 11, 14\}\ mod\ 15$
$\sqrt{4} = \{2, -2, 7, -7\} = \{2, 7, 8, 13\}\ mod\ 15$
In this case we can only get one square root of 1 in modulo 15 and one square root of 4 in modulo 15. However, if we get 4 for the square root of 1 in modulo 15 and 8 for the square root of 4 in modulo 15, they add up to 12 and gcd(12,15) gives us 3, which is p since 15 = 3 * 5.
When we can only have one square root of a square in modulo n, we can pick two squares and get two square root of each in modulo n. There is a chance that the two square roots are in the form:
<x mod p, a mod q> and <-x mod p, b mod q>.
Thus, when we add them together, we get <0 mod p, (a+b) mod q>. This number and n's greatest common divisor is obviously p. Therefore, if we can only get one square root in modulo n, we can still factor n. Thus, the counter argument in the question is not a good counter argument.

4.
Let x be the least number of eggs in the basket.
According to the question, we have:
$x \equiv 1 \bmod 2$
$x \equiv 2 \bmod 3$
$x \equiv 1 \bmod 4$
$x \equiv 1 \bmod 5$
$x \equiv 5 \bmod 6$
$x \equiv 3 \bmod 7$
$x \equiv 5 \bmod 8$
We can tell that 2,3,4,5,6,7,8 are not all relatively prime. So, at the first place we realize that having the last four equations is the same as having all the 7 equations. Thus, we eliminate the first 3 equations. Then, 6 and 8 are not relatively prime, but we can change these two equations into one equation modulo 24 since 24 is the least common multiple of 6 and 8.
After that, we have:
$x \equiv 1 \bmod 5$
$x \equiv 3 \bmod 7$
$x \equiv 5 \bmod 24$
The least common multiple of 5,7,24 is 840. Then, we know:
$168^{-1} \equiv 2 \bmod 5$
$120^{-1} \equiv 1 \bmod 7$
$35^{-1} \equiv 11 \bmod 24$
Then, we know:
$x = (1\times168\times2 + 3\times120\times1 + 5\times35\times11) \bmod 840 = 101$
Thus, there are at least 101 eggs in the basket.