CS 161 – Computer Security
Instructor: Tygar
15 September 2014

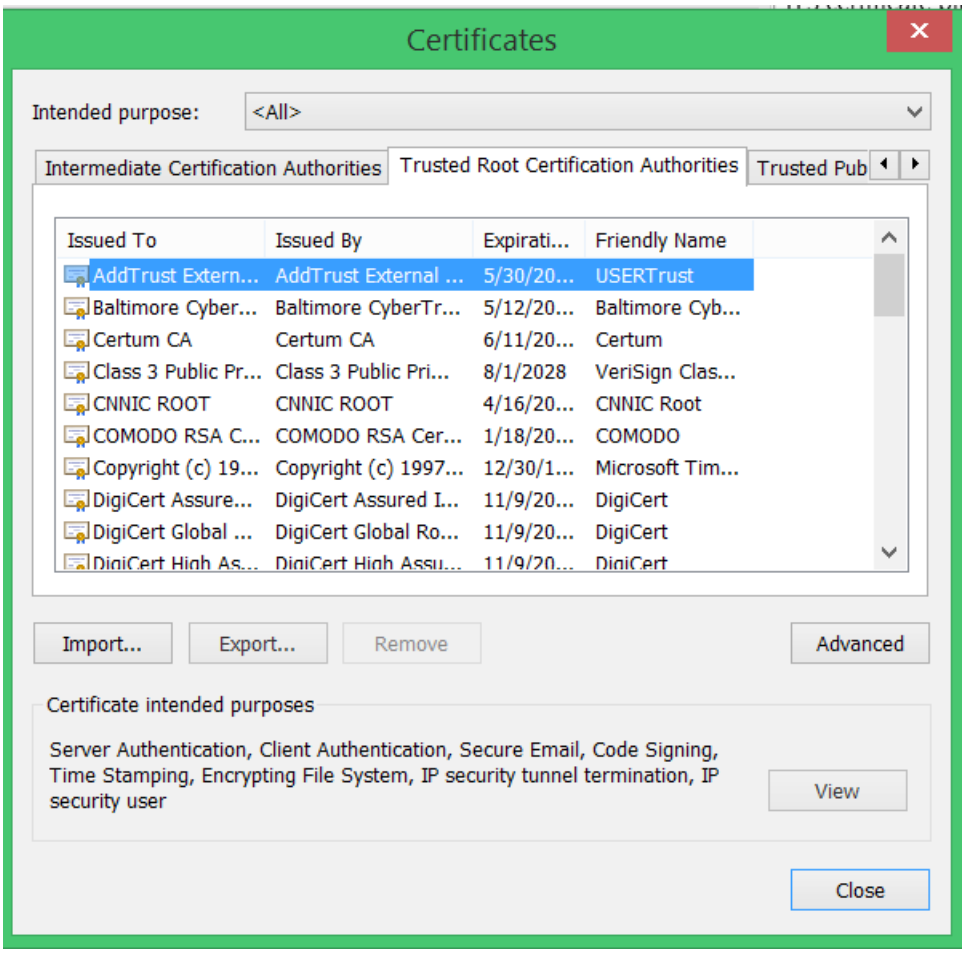
Homework 1 Answer Set

Notes

- Homework 1 is due on 15 September 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- It is possible to answer all questions relatively briefly. Please limit your answer to each question to a half-page at most.
- This homework should be submitted via "Gradescope." We will shortly post instructions for submitting the homework on our Piazza class page.

1. Read the articles here: bit.ly/cnnic-breach and bit.ly/cnnic-breach2. This homework needs to be done on a fresh virtual machine Windows instance (or a completely clean copy of Windows). Download and install a clean copy of Internet Explorer 11. Does CNNIC appear in its signed certificates? Now go to https://cnnic.cn – now does CNNIC appear in its approved certificates now? (Include a screen shot.) What does that tell you about how Internet Explorer 11 handles certificates? What is the security risk in using Internet Explorer 11?

Internet Explorer 11 dynamically loads root certificates, so CNNIC does not originally appear on the list, but it is inserted after visiting https://cnnic.cn. This means it is not possible for a user to review the list of approved certificates and exclude those that he or she does not trust.



2. When RSA is used with encryption key $(e,n)=(11,5352499)$, the ciphertext received is

   195125 3886883 4748558

   (each block was encrypted successively). What was the plaintext? (Hint: WolframAlpha can help with calculations)

   Factor $5352499=1237\times 4327$. *Note* $\varphi(n)=5346936$. *Solving for* $11d\equiv 1(mod\,\varphi(n))$ *yields* $d=4860851$. *The plaintext is*

   4491763 32 23

3. Consider the following counter-argument against the proof that breaking Rabin signatures was equivalent to factoring: *To factor, it is necessary to take two square roots modulo n. But now, suppose that we only produce one square root, not two. For example, maybe we always produce the square root that is lowest in value. Since we only have one square root, we cannot use the method shown in class to factor.* Is this a good counter-argument? Why or why not.

It is a bad counter-argument. We can generate two square roots by picking a random r *and then calculating* $s=\sqrt{r^2 \pmod n}$. *With 50% probability,* $r \neq \pm s \pmod n$.

4. There are eggs in a basket. When the eggs are taken out two at a time, there is one egg left. When the eggs are taken out three at a time, there are two eggs left. When the eggs are taken out four at a time, there is one egg left. When the eggs are taken out five at a time, there is one egg left. When the eggs are taken out six at a time, there are five eggs left. When the eggs are taken out seven at a time, there are three left. When the eggs are taken out eight at a time, five are left. What is the least number of eggs in the basket? Use the Chinese Remainder Theorem to solve this problem, and show your work. (Note that 2, 3, 4, 5, 6, 7, and 8 are *not* all relatively prime.)

   We use 3, 5, 7 and 8 which are relatively prime. We need to find m *such that* $m \equiv 2 \pmod 3, m \equiv 1 \pmod 5, m \equiv 3 \pmod 7, m \equiv 5 \pmod 8$. *CRT yields* $m=101$.