CSEP 590A: Practical Aspects of Modern Cryptography Winter 2011

Assignment #5

Due: February 17, 2011

1) Suppose that ORCA cards and readers are only capable of symmetric (e.g. AES) encryption but you want each card to have its own symmetric key for communications with readers. Although you don't like it, you are assured that there is enough physical security around the readers so that they can all share a single key.

   Describe a design wherein each card can use its unique symmetric key to communicate securely with any reader.

2) Now let's suppose that ORCA cards are capable of public key encryption. Each card will have its own public-private key pair, and readers will perform revocation checking whenever interacting with a card. We'll assume that a CRL is distributed once a day to all the readers, and that there are approximately 1,000,000 ORCA cards in distribution in Puget Sound.

   Assume that the loss rate for transit cards like the ORCA is approximately 1% per month. In the steady state approximately how big would the CRL need to be for ORCA cards if the CRL has to have an entry for every card revoked within the past two years? (You may assume that a CRL requires 512 bytes of fixed information plus 36 bytes of storage per revocation entry when ASN.1 encoded.)

3) Continuing the scenario in Problem 2, let's assume Sound Transit rolls out CRLs for public-key based ORCA cards and runs into a few problems. First, the readers in buses have very slow uplink interfaces and it takes too long to download a new "full" CRL every day into the reader. So instead of downloading an entire CRL every time, Sound transit asks you to design an alternative data structure that allows for incremental updates (so the amount of information uploaded to each reader every night is proportional to the number of entries that change in the "CRL").

   For your first attempt, you propose a scheme where each evening the CA at ORCA Central issues a new "incremental" CRL listing just the cards that have been revoked that day. Each evening, this new CRL is uploaded to the readers and the CRL that is now two years old is expired & erased. This scheme gets the right information onto each reader, but it means that the reader has to search 730 (2x365) CRLs each time it does a revocation check, which turns out to be very slow. So Sound Transit asks you to try again.

Design an alternative data structure for holding CRL information on each reader that has the following properties, where m is the total number of revoked cards in the data structure and n is the number of additions and deletions made to the data structure in a single day:

a. Each day's incremental updates involve only $O(n \log m)$ modifications to the data structure.
b. Searching the "CRL" for an entry takes $O(\log m)$ time.
c. Like a "regular" CRL, the data structure is always integrity-protected with a digital signature from the CA.

4) A company has a president and two vice-presidents. The corporate rules require that payments over \$10,000 require either the president's signature or the signature of both vice-presidents. The president already has a certified RSA key pair on public key N with the usual exponent of $e = 65537$ and the associated private exponent of d. As a dabbler in cryptography, the president computes private exponents d_1 and d_2 such that $m^{3d_1} \bmod N = m$ and $m^{5d_2} \bmod N = m$ for $0 \leq m < N$.

Show that $m^{15d_1d_2} \bmod N = m$ for $0 \leq m < N$.

The president then gives one of each of d_1 and d_2 to each of the vice-presidents and signs a new certificate on the same N with public exponent $e = 15$. The president's instructions are that if the vice-presidents want to jointly sign a payment m, they should each apply their decryption exponents to m to produce a valid signature against the verification exponent of $e = 15$.

Describe why this is a *bad* idea.