CSEP 590E: Practical Aspects of Modern Cryptography

Homework #2 Due: 6:30pm Oct 18, 2016

1. Show that
   a. If P and Q are distinct primes and $X \bmod P = Y \bmod P$ and $X \bmod Q = Y \bmod Q$, then $X \bmod (PQ) = Y \bmod (PQ)$.
   b. If P and Q are distinct integers and $X \bmod P = Y \bmod P$ and $X \bmod Q = Y \bmod Q$, it is *not* always true that $X \bmod (PQ) = Y \bmod (PQ)$.

2. From Fermat's Little Theorem, we know that for all primes P and integers Y, it is true that $Y^P \bmod P = Y \bmod P$. Use this together with mathematical induction to show that for all primes P, integers Y, and positive integers k, $Y^{k(P-1)+1} \bmod P = Y \bmod P$. [If you use a version of Fermat's Little Theorem other than the one given here, you may need to handle the case where $Y \bmod P = 0$ separately.]

3. Combine your results from the first two problems to prove the RSA equation: for all distinct primes P and Q, integers Y, and positive integers K, it is true that $Y^{K(P-1)(Q-1)+1} \bmod (PQ) = Y \bmod (PQ)$.

4. RSA has a multiplicative structure that enables some limited computations to be performed on encrypted data.
   a. Show that if $Z_1 = Y_1^X \bmod N$ and $Z_2 = Y_2^X \bmod N$, then $(Z_1 Z_2) \bmod N = (Y_1 Y_2 \bmod N)^X \bmod N$.
   b. Find a (plausibly) one-way function f (remember we don't even know that any one-way functions exist – we just have functions that we don't know how to invert) which has additive structure such that $f(X_1) \oplus f(X_2) = f((X_1 + X_2) \bmod M)$ for some appropriate operator $\oplus$ and modulus M. Be sure to specify your M and any other modular restrictions you may include.

5. With the ordinary *unauthenticated* Diffie-Hellman key exchange protocol, Alice randomly generates a and sends Bob $A = Y^a \bmod P$ and Bob randomly generates b and sends Alice $B = Y^b \bmod P$. (Prime P and integer Y are public parameters agreed to in advance or as part of the exchange.) An *authenticated* version of the Diffie-Hellman protocol starts with Alice holding a secret key $\tilde{a}$ and a signed certificate attesting to her public key $\tilde{A} = Y^{\tilde{a}} \bmod P$ and with Bob holding a secret key $\tilde{b}$ and signed certificate attesting to his public key $\tilde{B} = Y^{\tilde{b}} \bmod P$. However, this authenticated version does not achieve forward secrecy because the key exchanged between Alice and Bob never changes. An authenticated and forward secret protocol can be produced by combining both ephemeral (temporary) keys and permanent certified keys in each instantiation of the protocol and forming $K = A^{\tilde{b}}\tilde{A}^b \bmod P = B^{\tilde{a}}\tilde{B}^a \bmod P$ as an ephemeral shared key.

    a. Would the protocol offer forward secrecy if $K = \tilde{A}^{\tilde{b}}A^b \bmod P = \tilde{B}^{\tilde{a}}B^a \bmod P$? Why or why not?
    b. Describe how to use the Diffie-Hellman protocol to exchange a key with one-sided authentication if Alice has the certified public key $\tilde{A} = Y^{\tilde{a}} \bmod P$, but Bob has no certified public key.