Project 2: Implementation of Digital Signature Algorithm(s)

Due by June 2, 2010

This project asks you to develop digital signature algorithms (DSAs) based on the understanding of encryption/decryption by RSA and ElGamal strategies. For more details, refer to Chapter 9 of the Cryptography textbook by Trappe and Washington, 2006.

In the initialization step,

1. Alice selects a prime $q = 997$ (10-bit long) and she finds another prime $p = 23929$ (16-bit), where $q|(p-1)$ and $p = 24q + 1$.

2. Alice picks up $g = 7$ which is a primitive root $(mod\ p)$, then she computes $\alpha = g^{(p-1)/q} \equiv 20424\ (mod\ p)$.

3. Alice chooses a *secret* $a = \mathbf{127}$ and computes $\beta \equiv \alpha^a \equiv 1483\ (mod\ p)$.

4. Alice publishes $(p, q, \alpha, \beta) = (23929, 997, 20424, 1483)$ and keeps $a = \mathbf{127}$ secret.

5* For steps $\mathbf{2} \sim \mathbf{4}$, $g = 19$, $g = 41$, or other primitive roots $(mod\ p)$ might be used.

For the signing process, Alice signs a message m by the following procedure:

S1. Select a random, secret integer $\mathbf{k}$, such that $0 < \mathbf{k} < q - 1$.

S2. Compute $r = (\alpha^k\ (mod\ p))\ (mod\ q)$

S3. Compute $s = (k^{-1}(m + ar))\ (mod\ q)$

S4. Alice sends the signature (m, r, s) for m to Bob.

For the verification process, Bob verifies the signature by the following procedure:

V1. Bob downloads Alice's public information $(p, q, \alpha, \beta) = (23929, 997, 20424, 1483)$.

V2. Compute $u_1 \equiv s^{-1}m\ (mod\ q)$, and $u_2 \equiv s^{-1}r\ (mod\ q)$.

V3. Compute $v = (\alpha^{u_1}\beta^{u_2}\ (mod\ p))\ (mod\ q)$

V4. Bob accepts the signature iff $v = r$.

Your work is to write a set of programs to

(1) select public keys (p, q, α, β) (dsa-ini.c is ready for your reference).

(2) sign a message m $(0 < m < q - 1)$ with a random k and report (m, r, s).

(3) verifies (m, r, s) for m based on the public key (p, q, α, β).

Select k in step (S1.) from your student #, for examples, use $k = \mathbf{244}$ from id=9562**244**, and use $k = \mathbf{515}$ from id=9865**515**. Report the signatures of (m_1, r_1, s_1) with $m_1 = 511$ and (m_2, r_2, s_2) with $m_2 = 911$, respectively. Also, verify your results.

♣ Can you extend your program for 160-bit q and 1024-bit p?