**Department of Electrical and Computer Engineering**

**University of Massachusetts Dartmouth**

**ECE 489/549 Network Security Fall 2014 Prof. Hong Liu**

**Homework #7: Authentication: Protocols**

1. [Confidentiality & Integrity] In what order should the signature function and the confidentiality function be applied to a message, and why? Demonstrate your choice by applying a concrete encryption algorithm such as DES or RSA.

Hint: You can have two choices as follows.

1. Signature( Confidentiality(M, Kc), Ks )
2. Confidentiality( Signature(M, Ks), Kc )
3. [Digital Signature] It is tempting to try to develop a variation on Diffie-Hellman that could be used as a digital signature. Here is one that is simpler than DSA and that does not require a secret random number in addition to the private key.

**Public elements:**

q prime number

α α < q and α is a primitive root of q

**Private key:**

X X < q

**Public key:**

Y = αX mod q

To sign a message M, compute h = H(M), the hash code of the message. We require that gcd(h, q-1) = 1. If not, append the hash to the message and calculate a new hash. Continue this process until a hash code is produced that is relatively prime to (q-1). Then calculate Z to satisfy Z×h ≡ X mod (q-1). The signature of the message is αZ.

To verify the signature, a user verifies that Y = (αZ)h = αX mod q.

1. Show that this scheme works. That is, show that the verification process procedures an equality if the signature is valid.
2. Show that the scheme is unacceptable by describing a simple technique for forging a user’s signature on an arbitrary message.