T-79.159 Cryptography and Data Security **Spring 2004**
Tutorial 7
Thursday 18.3.2004 14.15, room T3.
Markku-Juhani O. Saarinen `<mjos@tcs.hut.fi>`

1. Try to invent a simple identification protocol based on a shared secret K where the actual secret is not transmitted. Note that e.g. `telnet` password authentication does not satisfy this requirement since the password is transmitted in clear.

   In the protocol Alice wishes to authenticate herself (i.e. prove knowledge of the shared secret K) to Bob. Use only symmetric cryptography – a hash function or a block cipher. How many messages are required in the protocol ? What if Bob also wishes to authenticate himself to Alice ?

2. The purpose of this exercise is to illustrate how (and why) Schnorr-like Subgroup-DH - based cryptographic algorithms work.

   The (U.S. Federal) Digital Signature Algorithm (DSA) uses the following parameters:

   - Public primes p, and q, $q \approx 2^{160}$, $p \approx 2^{1024}$, where q divides $p - 1$.
   - A public generator g of order q: $g^q \equiv 1 \pmod{p}$.
   - A randomly chosen private key x, $0 < x < q$ and corresponding public key $y = g^x \bmod p$.
   - A secret quantity k, $0 < k < q$, which is randomized for each message to be signed.

   To generate the signature (r, s) from a message $m = \text{SHA-1}(M)$ (i.e. actually the SHA-1 hash of the message), we pick a random k, $0 < k < q$, and set:

   $$r = (g^k \mod p) \bmod q$$
   $$s = (k^{-1}(m + xr) \mod p) \bmod q.$$

   To verify the signature (r, s), given the message m and the public parameters p, q, y, we set:

   $$u_1 = (ms^{-1}) \bmod q$$
   $$u_2 = (rs^{-1}) \bmod q$$
   $$v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q.$$

   The signature is valid if $v = r$. Please show why we would expect this algorithm to work (i.e. prove the correctness of signature verification) !