

## Homework #5

Due November 30, 2011, beginning of the class

1. Question 4, the midterm exam of Fall 2010.
2. Compare the RSA and ElGamal signature schemes' performance in terms of
  - efficiency of the verification operation,
  - ability to pre-compute most of the signature operation in advance.

Which scheme should be preferred for an SSL certificate? Which scheme should be preferred for a real-time authentication protocol on a restricted device—e.g., an RFID tag on an electronic passport? Explain why.

3. For this exercise assume the following notation for Schnorr and DSA signatures:  
Common parameters: Large prime  $p$ , 160-bit prime  $q|(p-1)$ ,  $g \in \mathbb{Z}_p^*$  of order  $q$ .

Schnorr:

$$\begin{aligned}v &= g^k \bmod p \\ r &= H(M||e) \\ s &= (k - r\alpha) \bmod q\end{aligned}$$

DSA:

$$\begin{aligned}v &= g^k \bmod p \\ r &= v \bmod q \\ s &= k^{-1}(H(M) + r\alpha) \bmod q \\ (H(M) &\equiv sk - r\alpha \pmod{q})\end{aligned}$$

- (a) Compare the Schnorr and DSA encryption schemes in the ways they
  - reduce  $r$  to 160 bits
  - incorporate  $M$  into the signature.
- (b) While remaining as close to the original signature equations as possible, convert DSA into an Schnorr-like signature scheme, and Schnorr into a DSA-like signature scheme. Explain your reasoning and the choices you made. (Hint: Think of a Schnorr-like scheme as an ElGamal variant that uses  $(1, s, r)$  as the coefficients in the signature equation instead of  $(H(M), s, r)$ .)