Introduction to cryptography

ESISAR IR&C 2019/2020

Cyril Hugounenq

All useful documents on Pari-GP can be found at **https://pari.math.u-bordeaux.fr/doc.html**

1 RSA in practice

1. Implement a pair of functions:

   - RSA_OAEP_enc(m,N,e)
   - RSA_OAEP_dec(c,N,d)

   where $n = 768$, $k = 256$ and G and H belong to the SHA2 family.
   Note: the encryption function should check the size of its inputs.

2. Implement a pair of functions:

   - RSA_PSS_sign(m,N,d)
   - RSA_PSS_verify(m,s,N,e)

   where $k = 256$, H=SHA256 and G=SHA384.
   Note: both functions should check the size of their inputs.

2 On the difficulty of solving the discrete logarithm over prime fields

1. Use the *ploth* function to display the first 200 values of $g^x \mod p$ for some integer x and a prime p on 768-bit. Note the seemingly random behaviour of the function to get an idea of the difficulty of solving the discrete logarithm.

2. Using the *znlog* function, show the empirical difficulty of solving DLP depending on the smoothness of the order of the group. What should be the structure of our prime?

3 El-Gamal and DSS

1. Implement a function *gen_DLP_parameters(g,p)* returning a pair of public/private keys [pub,priv]

2. Implement a function *ElGamal_enc(g,p,pub,M)* returning a ciphertext [K,C]

3. Implement a function *ElGamal_dec(g,p,priv,K,C)* returning a plaintext M

4. *Bonus:* Implement the signature scheme *DSS_sign(g,p,priv,M)* and *DSS_verify(g,p,pub,M,Kr,Km)* using H=SHA256