Introduction to cryptography

ESISAR IR&C 2020/2021

Hugouneng Cyril

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

1 Getting familiar with Pari-GP: Generating primes

1. Start Pari-GP with the command **gp** and import file *rsa.gp* by entering *read(rsa)* or \r *rsa.gp*

2. Use *gen_prime* to generate a prime number on 512 bits. Using the User's guide, explain why the generation is so fast.

3. Is it secure to use such a function to generate a long term RSA key? Modify the existing code if necessary.

4. In practice, NIST recommends stronger assumptions on primes used for RSA

   - **Strong prime:** p is a strong prime iff $\frac{p-1}{2}$ is also prime
   - **RSA prime:** p is a RSA prime iff $\frac{p-1}{2}$ is a strong prime
   - Implement a function *gen_RSA_prime(b)* which generates a RSA prime on exactly b bits

5. *Bonus:* Implement a function counting the number of primes lower than a bound m and check empirically that this number is close to $\frac{m}{log(m)}$

2 Generating RSA parameters

1. Implement a function *gen_RSA_parameters(b)* which generates a set of RSA parameters on b-bits and returns $[N, e, d]$.

2. Implement a function *RSA_encrypt(M,N,e)* which encrypts a message M using a public key $[N, e]$

3. Implement a function *RSA_decrypt(C,N,d)* which decrypts a message C using a private key $[N, d]$

4. *Bonus:* Using the gp function *chinese*, implement a function *RSA_sign_CRT(M,N,d_p,d_q,p,q)* which signs a message M using a private key $[N, d \mod p-1, d \mod q-1, p, q]$ (modify the function *RSA_gen_parameters* accordingly). The signature value shall be $S = M^d[N]$.

3 Attacks on RSA

1. Implement a function *factor_from_phi(N,phi)* which factors N given $\varphi(N)$.

2. Implement a function *factor_from_d(N,e,d)* which factors N given e and d.

3. Implement a function *broacast_attack($M^3 \mod N_a, N_a, M^3 \mod N_b, N_b, M^3 \mod N_c, N_c$)* which recovers M.

4. Implement a function *wiener_attack(N,e)* which recovers d assuming that $d < \frac{1}{3}N^{\frac{1}{4}}$.