CRYPTOGRAPHY

MESIGI3906
PRIME NUMBERS WITH GPG/OPENSSL/GMP

JOHN CAGNOL / AMAURY DARSCH
DER CALCUL SCIENTIFIQUE / DER GÉNIE INFORMATIQUE

AGENDA

- Prime numbers
  - Generation with GPG
  - Testing with OpenSSL
- GMP
  - Multi-precision arithmetic
  - Simple conversion and predicate

PRIME NUMBERS

- Large prime numbers are essential with certain cryptographic operations
- OPENSSL
  - Generation : impossible
  - Verification : possible [decimal]
    - openssl prime [num]
- GPG
  - Generation : possible [hexadecimal]
    - gpg –gen-prime 1 [bits]
  - Verification : impossible

GMP

- GNU multi-precision library
  - Fast large integer arithmetic
- Standard operations
  - Usual operations, conversions
  - Modular arithmetic
  - Primality testing and generation
- Available on most platforms in native mode
  - gcc [file to compile] -lgmp
  - Can crash if badly compiled or installed

TRANSFORMATION GMP

```
/*
 * ios: simple i/o demo with gmp
 *      ESILV S9 2008-2009
 *      John Cagnol - Amaury Darsch
 */

#include <stdlib.h>
#include <stdio.h>
#include "gmp.h"

/*
 * usage: print a usage message
 */

static void usage () {
  fprintf (stderr,
           "usage: ios number\n");
  exit (1);
}
```

```
/*
 * main program
 */

int main (int argc, const char** argv) {
  // declarations
  mpz_t n;

  // check number of arguments
  if (argc != 2) usage ();

  // initialize and load
  mpz_init (n);
  if (mpz_set_str (n, argv[1], 0) != 0)
    usage ();
  // print value
  mpz_out_str (stdout, 10, n);
  fprintf (stdout, "\n");

  // everything is fine
  return 0;
}
```

```
gcc -Wall -o gmp-ios gmp-ios.c -lgmp
```

PREDICATE WITH GMP

- GMP can be used to test if a number is prime :
  - mpz_probab_prime
- Exercise
  - Write a program to test if a number is prime
  - Find the mean distribution of prime numbers between two bounds
  - Generate a random number and check for its primality. How many trials are needed before finding a prime number.
  - How long does it take to find a probable prime?