

# Cryptography and security

Pierre Colson

## Contents

General . . . . .	1
Diffie Helman . . . . .	1
RSA . . . . .	1

Markdown version on *github*

## General

- $b \in \mathbb{Z}_p^*$  has a square root if and only if  $b^{\frac{p-1}{2}} \mod p = 1$

## Diffie Helman

- We check that  $X$  and  $Y$  are in  $\langle g \rangle$
- Use a KDF to fix bad distribution of  $g^{xy}$
- We check the lower order  $X \neq 1, X^2 \neq 1$
- If  $n = pq$  then  $\mathbb{Z}_n$  ring is isomorphic to  $\mathbb{Z}_p \times \mathbb{Z}_q$  and  $\mathbb{Z}_n^*$  ring is isomorphic to  $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$

## RSA

- Square and multiply algorithm to compute  $x^e$  or  $x^d$
- Primality test : Verify that a number is prime
- To check if a number is coprime is another one use euclid algorithm
- To compute the inverse of an elem use extended euclid algorithm
- $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$
- We can compute square root of  $n$  in  $\mathcal{O}(\log n)^3$