Cryptography and security

Pierre Colson

Contents

Markdown version on *github*
Compiled using *pandoc* and ***`gpdf`*** *script*

General

- $b \in \mathbb{Z}_p^*$ has a quare 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 wheck 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 os 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 $\mathcal{O}(\log n)^3$

Elliptic Curve

- All finite fields have a cardinality of form p^k where p is a prime number This prime number p is called the **characteristic** of the field.
- A **binary** field is a field with characteristic equal to 2
- Over a field $\mathbb{R}$, an elliptic curve with parameters a and b consists of a special point $\mathcal{O}$ called the *point at infinity* and the points (x, y) which are the solutions of the equation $y^2 = x^3 + ax + by$

- Elliptic Curve over a **Prime Field**
  - The **discriminent** is $\Delta = -16(4a^3 + 27b^2)$
  - The curve is **non-singular** iff $\Delta \neq 0$
  - We define the **j-invariant** $j = 1728\frac{4a^3}{Aa^3+27b^2}$, two isomorphic curves have the same j-invariant
- Elliptic Curve over a **Binary Field**
  - **Ordinary** curves are defined by two fieds elements denoted a_2 and a_6

$$E_{a_2,a_6}(\mathbb{K}) = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{K}^2; y^2 + xy = x^3 + a_2x^2 + a_6\}$$

  - We define the **j-invariant** $j = \frac{1}{\Delta}$
- Simple factoring method : Pollard's (also called $p - 1$ algorithm)
- **Elliptic Curve Method** (ECM) is the best method to find p when it is small
- **ECDH** key exchange protocol is tha variant of Diffie-Hellman protocol working over an elliptic curve group
  - We have two participant U and V using the same subgroup of order n genrated by some point G over an elliptic curve.
  - They both select their secret key $d_U, d_V \in \mathbb{Z}_n^*$
  - They compute their public key $Q_U = d_U.G$ and $Q_V = d_V.G$ which are point and exchange them.
  - Then, they both check that the received publoc key is actually a point of the curve which is generated by G, different from the point at infinity, and that its order is a factor of n.
  - They both compute the a point P, either by $P = d_U.Q_V$ or by $P = d_V.Q_U$
  - They take the first coordinate x_p of P and convert it into a byte string Z
  - Finally they compute $K = KDF(Z)$