Homework #4
Elliptic Curves

CNS Course Sapienza

Riccardo Prinzivalle, 1904064

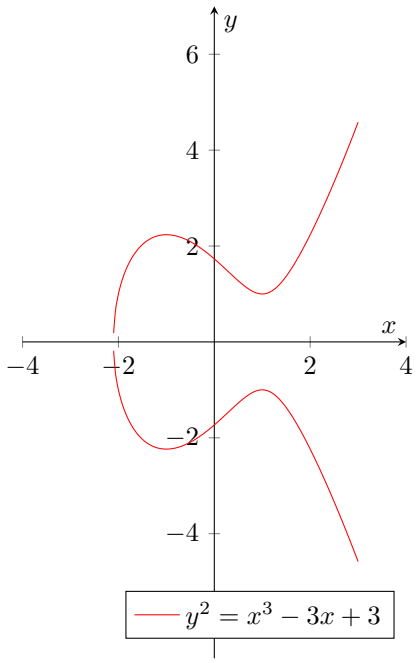
November 20, 2020

1 Homework Goal

This homework contains a basic introduction on Elliptic Curves (EC), the general idea on the math basis, the Discrete Logarithm Problem with EC and the practical utilize of EC in cryptography.

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer Factorization	RSA	1024	3072	7680	15360
Discrete Logarithm	DH, DSA, Elgamal	1024	3072	7680	15360
Elliptic Curves	ECDH, ECDSA	160	256	384	512
Symmetric key	AES, 3DES	80	128	192	256

Table 1: Key length comparison in public key and symmetric key algorithm



2 Mathematical background

3 Discrete Logarithm Problem with Elliptic Curves

(a) Core (b) Preprocessing

Figure 1: Mix columns base functions

4 Use of Elliptic Curves in Cryptography

5 Conclusion

Even if the implementation proposed is much slower than the standard library chosen as comparison, it works well and it does its dirty job. The code may not be much optimized or it can have been written in a better way but my knowledge in python is not so huge, but this was an opportunity to dust and improve my experience.