Homework #3
RSA

CNS Course Sapienza

Riccardo Prinzivalle, 1904064

November 20, 2020

1 Homework Goal

This homework contains an implementation of RSA algorithm based on major libraries for the mathematical functions, a comparison with the insecure *PyCryptoDome* RSA and with the *PyCryptoDome* AES.

2 RSA Implementation

3 RSA Comparison

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

4 Conclusion

After this brief introduction on elliptic curves, it is obvious why they have been widely adopted in many cases of asymmetric encryption: they use less bits for the same level of security, so are more efficient to compute and their base concepts are easier to visualize. As suggested on section **??**, EC can be easily used in hybrid encryption scheme, in the key exchange phase.

References

[1] C. Paar and J. Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Publishing Company, Incorporated, 1st edition, 2009.