Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Computational tools for problem solving

Lab list 4

Problem 1. Consider the RSA cryptosystem with public key

$$(n, e) = (135828482760150159223553231524924630769084223558056259571, 17).$$

Assume the following encoding of two letters into one number in $\mathbb{Z}_n$.

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

i) Use Fermat's factoring method to factor n as the product of two prime numbers.

ii) Compute $\phi(n)$.

iii) Using the extended Euclidean algorithm, compute the private key of this RSA cryptosystem.

iv) The ciphertext $c = 946002826551013430319305334276725656656150537082888843906$ was obtained by encrypting the encoding sequence of a message m. Find m.