RSA

p; **q**	**3**	**11**
n = pq	33	
f = (p-1)(q-1)	20	
e coprimo minore di **f**	**7**	
d tale che de≡ 1 mod (p-1)(q-1)	**3**	
Chiave pubblica (n, e)	33	7
Chiave privata (n, d)	33	3

Primi 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

MCD(e;f) 1

Metodo Euclide (prendere la colonna 2 quando la colonna 1 è uguale a 1)

20	0	
7	1	2
6	-2	1
1	3	6
0	-20	#DIV/0!
#DIV/0!	#DIV/0!	#DIV/0!
#DIV/0!	#DIV/0!	#DIV/0!
#DIV/0!	#DIV/0!	#DIV/0!
#DIV/0!	#DIV/0!	#DIV/0!
#DIV/0!	#DIV/0!	#DIV/0!

se **d<0** -> d= d + f

Messaggio (0<**m**<n)	15	
Codifica **c**	27	$c = m^e \bmod n$
Decodifica	15	$m = c^d \bmod n$