RSA Cryptography

Physics II: Modern Physics

College of the Atlantic

1. What is $2^5 \mod 14$?
2. What is $11^5 \mod 14$?
3. Do the following problems as quickly as you can. Use a calculator.
   (a) What is 3137×5419?
   (b) The number 6992477 is the product of what two prime numbers?
   (c) The number at the bottom of the page is the product of what two prime numbers?
4. Calculate the following: $\phi(10), \phi(11), \phi(12), \phi(13), \phi(14)$, where ϕ is Euler's totient function.
5. What is $\phi(143)$?
6. Encrypt and then decrypt the message `LEG` using $e = 5, n = 14$, and $d = 11$.
7. Let $p = 3, q = 11$. We'll go though the steps of generating keys:
   (a) Compute N
   (b) Compute $\phi(N)$
   (c) Show that $e = 7$ satisfies the conditions on 3
   (d) Find the smallest possible d
   (e) Use the public key to encrypt the message "2"
   (f) Use the private key to decrypt the encrypted message

```
69495853675869655870565854535853575848655856575849515854555857565868665867525848565851695865
51585549585267585552585555585265584855585350587052585256585266586951586650585654586853586670
58705558706958525258685358675258536958535358535158705758684958516758516558675358494958555558
56575855695855505868545865535853555866695865525857495854535857485856575851505851575855705849
69585766586653586565586665585657585670586566585469586968584949585570586569585054585655586551
58655058485758576758676958525658655258537058506758486558546858555158695058527058675458576558
54485850535866545848485850656587495865485865535848575849535850535852545868705867545851685854
68586952585770585565584965586966586870586667587070585068585266585570586965585470585353587067
58654858655358566758535358655558545558686758555758675758706958705258535758685258695758705158
48575857535870565865555855515868695855505869705869525851515854675869665857495852685867535850
49586553586669585367585369585566585455585554585652585770585753585149584952585266586952586867
58655058486958485758536758697058666658505758526758694858555758506958705158676558486958705258
51535852565857575857685851555852495869505851685850535865675855665852655865705854675865655865
49587049586649585451585649585349586952584952587057586965586852584851586950586652586970585455
58675458565258666958536658695458575658576758705658666558485258565358685358536558575458544858
51685866555851675868665869695850535854495870695868555857555853545856525853555848705855575866
55585653585670585351587052584851584868586866586856587069584851
```