

RSA Cryptography

Physics II: Modern Physics

College of the Atlantic

1. What is $2^5 \pmod{14}$?
2. What is $4^{11} \pmod{14}$?
3. Calculate the following: $\phi(10), \phi(11), \phi(12), \phi(13), \phi(14)$, where ϕ is Euler's totient function.
4. What is $\phi(143)$?
5. 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?
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 through 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

2022 Version:

69495853675869655870565854535853575848655856575849515854555857565868665867525848565851695865
51585549585267585525855558526558485585350587052585256585266586951586650585654586853586670
58705558706958525258685358675258536958535358535158705758684958516758516558675358494958555558
565758556958555058685458655358535586669586552585749585453585748586575851505851575855705849
69585766586653586565586665585657585670586566585469586968584949585570586569585054585655586651
5865505848575857675867695852565865258537058506758486558546858555158695058527058675458576558
54485850535866545848485850655867495865485865535848575849535850535852545868705867545851685854
68586952585770585565584965586966586870586667587070585068585266585570586965585470585353587067
58654858655358566758535358665558545558686758555758675758706958705258535758685258695758705158
4857585753587056586555585551586869585505869705869525851515854675869665857495852685867535850
495865535866695853675853695855665854555855458565258577058573585149584952585266586952586867
5865505848695848575853675869705866665850575852675869485855758506958705158676558486958705258
5153585256585757585768585155585249586950585168585053586567585566585265586570585467586655865
49587049586649585451585649585349586952584952587057586965586852584851586950586652586970585455
58675458565258666958536658695458575658576758705658666558485258565358685358536558575458544858
51685866555851675868665869585053585449587069586855857555853545866525853555848705855575866
55585653585670585351587052584851584868586866586856587069584851

2024 Version:

238689706374670622423919080835282398556060102125400359069877071897361362172186169652171542431228364435545653630792059940761154593917449
745855362332365226168633636664432909573414037437239880041256050368142665604933159596108208447191518904567551155784698501460087061260050654778
752298909500832665894924771728092611537273276424541282621740154788367800564088109223647707718291106727400395747116497363148425597808614475427
607294847925002704017240990065338116671088419169778013648190893641198745828429729154765061782344190495696146824664830156640220506527890038855080
995598460093335673348552244506213093235365140967879239