

Math 314 - Fall 2024

Practice problems 4 (Euler's Theorem, Fermat Primality Test, Dixon's Factorization)

Quiz: April 24 2024

Cryptography succeeds when it's no longer the weakest link.

— Ron Rivest

Practice:

- (1) Compute $\varphi(55)$ and $\varphi(54)$.
- (2) Find $10^{122} \pmod{55}$ without using a calculator.
- (3) Find the decryption function $D(y)$ corresponding to the encryption function

$$E(x) \equiv x^7 \pmod{54}.$$

- (4) Compute $3^{14} \pmod{15}$. What does this tell you about the primality/compositeness of 15?
- (5) Use the fact that $17^2 = 289 \equiv 16 = 4^2 \pmod{91}$ to factor 91 using the factoring trick.