Agile Programming and Test-Driven Development

Important Dates

Rubric

$$D_K (E_K (M)) = E_K (D_K (M)) = M$$

RSA Encryption

$$\phi(n) = (p-1)(q-1)$$

$$1 < e < \phi(n)$$

$$ed \equiv 1 \pmod{\phi(n)}$$

з п. а. а

$$c \equiv m^e \pmod{n}$$

$$m \equiv c^d \pmod{n}$$

Cryptanalysis of RSA

$$d < \frac{n^{1/4}}{3}$$

LSB Image Stego

Figure 1: One of these is the original image of Lena and the other is hiding 32KB of secret data.

Steganalysis and Countermeasures

Reminder about Resource-Intensive Jobs

Libraries and Other Resources

GitHub

Final Report and Presentation

Individual Scores

$$\min\left(teamScore \times \sqrt{\frac{yourContribution}{100/|group|}}, 110\right)$$

Need More Information?

Important Legal Notice