CS181S – Systems Security Fall 2020

Problem Session 3: Encryption

Monday September 14, 2020

1. Write a program or script to decrypt a ciphertext. You may assume the ciphertext is encrypted with hybrid encryption using RSA-2048 and AES-256 in CBC mode and Base64 encoded. The ciphertext, RSA secret key, and encrypted AES key are available on the course website. The randomly-generated IV used during AES encryption is 0x5A27710DB8004E0C4CF00573F5665290.