CS 406 : Cryptography and Network Security Spring 2024

Lab 4 — PKEs and Signatures

Instructor: Manoj Prabhakaran *Lab TA:* Nilabha Saha

Challenge 1: Public Encryption

In this challenge, you are given the RSA-OAEP private and public keys of a user in `pub.pem` and `priv.pem` respectively. The flag encrypted using the user's public key is provided to you in `cipher.bin`. Decrypt the ciphertext to recover the flag!

Challenge 2: Is This Certified?

Who digitally certified `https://www.cse.iitb.ac.in`? The flag for this challenge is the Canonical Name of the issuer of the digital certificate of `https://www.cse.iitb.ac.in`, enclosed in `cs406{`$\cdots$`}`. Replace any spaces in the issuer name with underscores.
Note that for this (and only this) challenge, the flag accepted is case-insensitive.

Challenge 3: ECDSA Nonce Reuse

A nonce should only be used **once**. Repeating nonce across signatures can lead to disastrous consequences. In this challenge, you'll be given two signatures generated using the same nonce. You need to recover the nonce and in fact, the private key of the signer!
Note that once you recover the private key of the signer, you can easily forge signatures at will!

Challenge 4: EdDSA Variants

One of the several digital signature schemes is EdDSA. You can read a high-level simplified overview here. It is based on the Schnorr signature scheme covered in class.
In this challenge, you are provided with two insecure custom variants of EdDSA. Figure out how you can exploit these variants to forge signatures on arbitrary message, and the flag will be yours!