Tell me about your Friend I will Tell about You

Practocrypt CTF

Solve the CTF for Alice by finding the correct Bob

Initially all will get 500 points

- step 1: Enter the user id as the seed value
- step 2 Compute the sha3 digest by passing (seed||01) to the sha3_256 algorithm where seed and 01 value are encoded as bytes.
- step 3: Take only the first 16 bytes of the sha3 digest as IV
- step 4: Call AES CTR mode PRNG by passing seed and iv to get the random number output
- step 5: generate random 32 bytes out as an output of rng value and convert it to integer to get the ECC private key
- step 6: use this private key to generate the ECC public key
- step 7: To find your correct partner's keypair i,e public and private repeat the steps 1 to 6 by passing their user id as seed value
- step 8: Next you need to find the shared secret key using ECDH function and print the shared secret value in hex format

Captured FLAG1, You get 500 points

- step 9: To decrypt the cipher text, use aead_decrypt
  - key = obtained shared secret key
  - nonce = 12 bytes of 0's
  - aad = sha3_output with the partner's public key as input
- step 10: print the decrypted text value if the decryption is done correctly.
- Else repeat the process with different partner's id until you find the correct plain text
- Hint the decrypted plain text will in this format (correct-partner-id+_+correct-partner-name+r+s)

Captured FLAG2, You get 500 points

- step 11: Extract signature value r+s from the decrypted plain text.
- Hint the r+s value will be 128 hex characters 64 for r and 64 s

- step 12: verify this ECDSA signature using
  1. extracted r and s value and convert the hex value of r and s to integer values
  2. correct partner's public key
  3. The input message = correct-partner-id+_+correct-partner-name which you will get from the decrypted plain text
- step 13: print the result to complete the CTF