Secrets of Alice and Bob

Category: Cryptography, Forensics

Can you find what the shared secret between Alice and Bob is?
flag format: isfcr{shared_secret}

Author: `Arrow#1334`

Flag:
`isfcr{0xb33ac0fbec48b8cbca7cb82ff8800339f4023b88a710c3fc8bbaa420f5a1e1a5de159177fb49c331600dfb33dbeec09db85d229865f702d320237ba9484b9d4e3c8b374410282b2fe19c2a39ad21ed69424954d571667abd961b81a2a2733c2be8c635aafcc53b8a923d1d44c346585aa089816230504abecb94bcab367abf42}`

This challenge is based on the Diffie-Hellman Key Exchange with a little bit of forensics involved (i.e. knowing how to use tools like wireshark to analyse packet captures). Open the packet capture with wireshark > Right click on first packet > Follow TCP Stream. We can see all the values that have been communicated.

If you read and understand the encryption system from the wikipedia, you'll find out that you've been given everything you need to find the shared secret:

- Alice Public Key: `A`
- Bob Public Key: `B`
- Alice Private Key: `a`
- Bob Private Key: `b`
- Shared modulus: `p`
- Base: `g`

Everything is calculated the exact same way as in the wiki. We have:

- `A = pow(g, a, p)`
- `B = pow(g, b, p)`

The shared secret can be calculated in either of the two ways:

- `S = pow(A, b, p)`
- `S = pow(B, a, p)`

Both will yield the same value because it is the "secret" that is shared between Alice and Bob. Alice can find the secret using her private key and Bob's public key. Bob can find the secret using his private key and Alice's public key. No other person eavesdropping in the public channel can figure out the secret unless they know the private key of either Alice or Bob, or are performing a man-in-the-middle (MITM) attack.