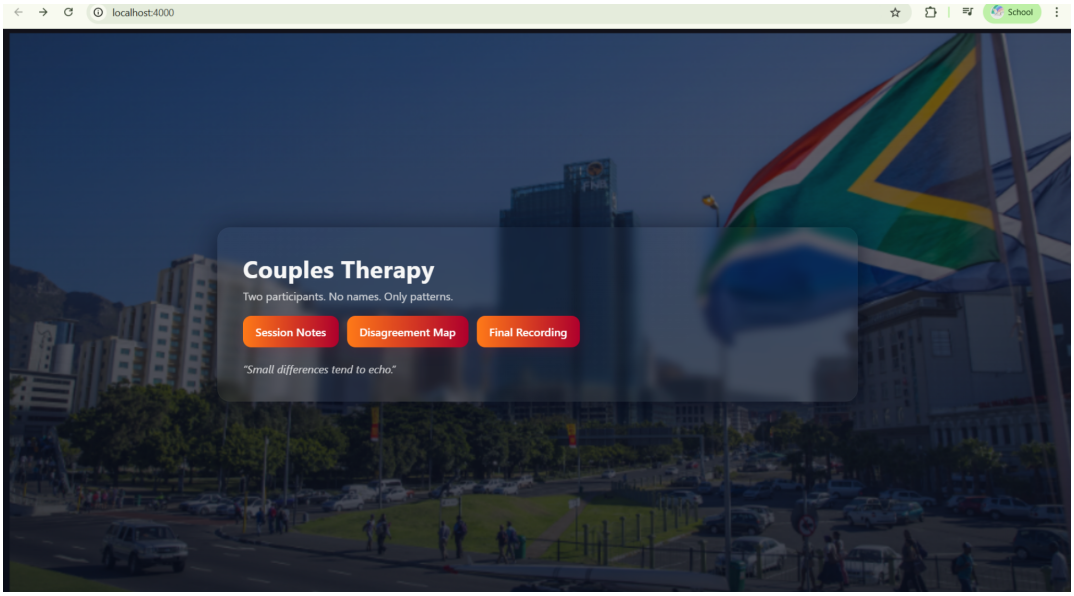
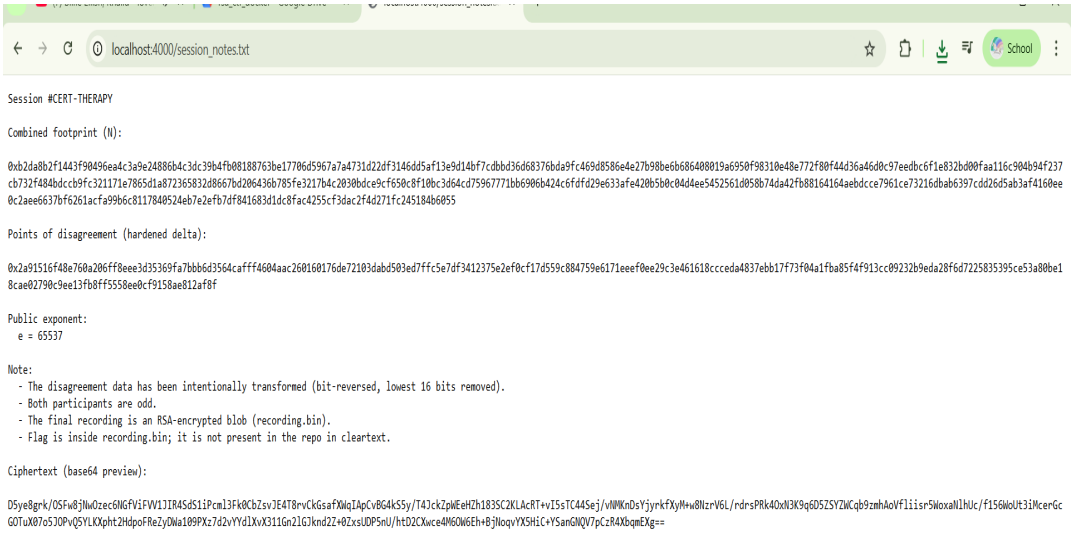
Couples Therapy – RSA + XOR Challenge Writeup

Couples Therapy is a cryptography challenge combining weaknesses in RSA key construction with an additional XOR obfuscation layer. The challenge provides partial information about the RSA key parameters, allowing recovery of the private key and decryption of the final encrypted recording.



Step 1: Inspect the Session Notes

By accessing the session notes, cryptographic parameters such as the RSA modulus (N), public exponent (e), and an obfuscated value related to the difference between the primes are revealed. These hints indicate that the RSA key is vulnerable to factorization.



Step 2: Reconstruct the RSA Primes

The challenge provides a transformed version of the value (p – q). After reversing the transformation (such as bit reversal and restoring truncated bits), the original difference can be approximated. Using the known modulus N and this difference, the RSA primes p and q can be mathematically recovered.

Note: Multiple valid mathematical approaches exist for this step, including quadratic solving or small brute-force adjustments for missing bits.

Step 3: Recover the RSA Private Key

Once p and q are known, Euler's totient $\phi(N)$ can be calculated. The private exponent d is then derived by computing the modular inverse of e modulo $\phi(N)$. This allows construction of the full RSA private key.

Step 4: Decrypt the Recording

Using the recovered private key, the file *recording.bin* is decrypted with RSA. The decrypted output does not immediately reveal the flag, indicating the presence of an additional obfuscation layer.

Note: Alternative cryptographic tools or libraries may be used for RSA decryption as long as the mathematical steps are correctly followed.

Step 5: Remove the XOR Obfuscation

The decrypted data is further processed using a repeating XOR operation. The XOR key is derived from the relationship between the RSA primes or their difference. After applying XOR, the plaintext becomes readable and reveals the flag.

Note: Players may derive the XOR key using different logical methods based on the provided hints.

Flag

LNMHACKS{black+white=rsa}