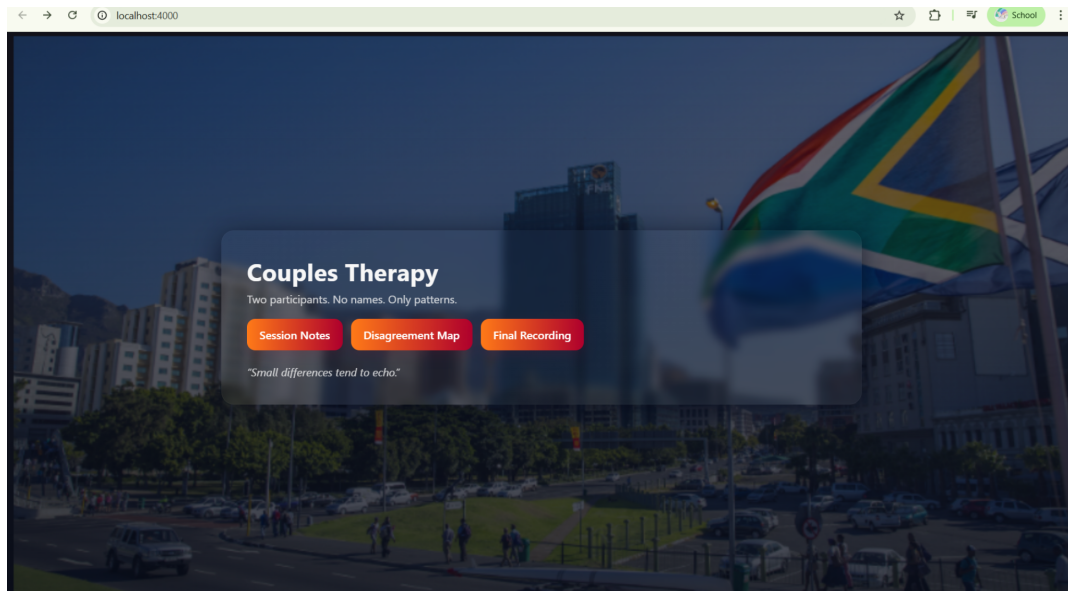


Couples Therapy – RSA + XOR Challenge Writeup

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.

```
localhost:4000/session_notes.txt

Session #CERT-THERAPY

Combined footprint (N):

0xb2da8b2f1443f90496ea4c3a9e24886b4c3dc39b4fb08188763be17706d5967a7a4731d22df3146dd5af13e9d14bf7cbbd36d68376bda9fc469d8586e4e27b98be6b686480819a6958f98310e48e772f80f44d36a46d8c97eedbc6f1e832bd00faa116c904b94f237
cb732f484bdcc9f321171e7865d1a8723658328866bd286436b785fe3217b4c28380dce9cf650c8f10bc3d64cd75967771bb6986b424c6fd29e633afe428b5b0c84d4ee5452561d858b74da42f688164164aebdcce7961ce73216dbab6397cdd26d5ab3af4168ee
0c2aee6637bf6261acfa99b6c8117840524eb7e2efb7df841683d1dc8fac4255cf3dac2f4d271fc245184b6d55

Points of disagreement (hardened delta):

0xa2a91516f48e760a206ff8ee3d35369fa7bb6d3564cafff4604aac260168176de72103dab583ed7ffc5e7df3412375e2ef0cf17d559c884759e6171eeef0ee29c3e461618ccceda4837ebb1773f04a1fba85f4f913cc89232b9eda28f6d7225835395ce53a80be1
8cae02790c9ee13fb8ff5558ee0cf9158ae812af0f

Public exponent:
e = 65537

Note:
- The disagreement data has been intentionally transformed (bit-reversed, lowest 16 bits removed).
- Both participants are odd.
- The final recording is an RSA-encrypted blob (recording.bin).
- Flag is inside recording.bin; it is not present in the repo in cleartext.

Ciphertext (base64 preview):

D5ye8grk/OSFw8jJm0Zec6MGV3FV1J1TR4SdS1Pcm13fk8CbZsvJE478rvCKgsaFMIqIqCvB64kSSy/T4JckZplMEhZ183SC2KLAcrT+vI5sTC44Sej/vNMKnDsYjyrkFXyH+w8lZrV6L/rdrsPrk40x13K9q605ZSY2WqB9zmh0vFl1iisSwoxa01lHuc/F156W0Ue3i1McerGc
G0Tux07o5JOPvQ5YLKXpht2HdpofReZyDNa1099PK7d2vYydlXvX311Gn21Gjkn2Z2+8ZxsUOP5nU/ht02Ckxced4M60M6EH+BjloqvYXSHc+YSanGQV7pCzR4XbqmEXg==
```

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}