FCS CTF 2022 Group 10 Cramer-Shoup Cryptosystem Challenge Attack Writeup

Author: Shaun Hin Fei 1005446

Based on the implementation, we can see that by implementing the check for w2 > x instead of w2 == v in the decryption algorithm and implementing x = large number instead of being randomly chosen greatly diminishes the security of the algorithm, as we are able to decrypt chosen ciphertexts, whereas the original cryptosystem is safe against such attacks.

Hence, we follow a CCA2 attack with access to the decryption oracle, and modify the ciphertext accordingly to produce a valid decryption of the chosen ciphertext, keeping in mind that our w2 has to pass the condition of being larger than the secret x. Thus, the attack works on probability and is solvable in about 1000 attempts.

The links which the attack is based on is as follows:

https://crypto.stackexchange.com/questions/20262/how-does-chosen-ciphertext-attack-on-elgamal-work