EVEN RSA CAN BE BROKEN???

In this problem, we are given an RSA-encrypted flag and the values of N and e. Normally, this would not be sufficient to decrypt the flag.

The program uses different RSA keys each time the program is connected. Even though the ciphertext changes each time, some of the RSA keys share a common factor of a prime number. This is because of poor random numbers in key generation, which goes against one of the basic assumptions of RSA.

When we are given an RSA key pair that shares a common factor of a prime number, we can use the greatest common divisor of the key pair to determine the prime number shared by the pair of keys. Once we determine this prime number, we can factor the key completely.

Once we determine the private key, we can then use RSA decryption to determine the original flag.

The key thing to learn from this problem is that cryptography is only as good as its implementation.