Wiener Attack + Factoring n given d

October 7, 2023

1 Introduction

Honestly looking at this again months after completing the challenge I'm not sure I solved it in the intended way - did it simply require a common modulus attack (as in the "twin" challenge)? Anyways, if so I really took the scenic route here, mounting Wiener's attack AND factoring n given the secret exponent d.

What we have given ("chall.py", "ciphers", "key1.pem", "key2.pem") is a message, split in two, and each of the two parts encrypted using one of the keys. The two keys share the same modulus n, but have different values for e. So regarding my remark above, unsure if a common modulus attack would have been possible since the two keys were used to encrypt different messages rather than the same. I used Wiener's attack to break "key1.pem" (see the additional document "wiener.tex"/"wiener.pdf" for details), and then factored n using the private exponent d_1.

2 Theorem of Secret Parameters: Break RSA using d

The *Theorem of Secret Parameters* states that given one entry of the private key (p,q,$\phi(n)$,d), and the public key, we can efficiently compute the full private key.

We know that by construction, $e \cdot d - 1 = x \cdot \phi(n)$ (d is the multiplicative inverse of e modulo $\phi(n)$).

Begin with the observation that since p, q are odd, $\phi(n) = (p-1)(q-1)$ is a product of two even numbers and thus itself even. We can thus write

$$\begin{aligned} e \cdot d - 1 &= x \cdot \phi(n) \\ &= 2^s \cdot k \end{aligned}$$

I.e., we have decomposed $e \cdot d - 1$ into s, its so-called multiplicity of two (the power of two in its prime factorization) and k, its odd part.

Now we will repeat the following procedure until we have found a factor of n:

1. Pick a random value $0 < a < n$.
2. Check if $gcd(a, n) > 1$. Since $n = pq$, the only greatest common divisor any number can share with n is $\in \{1, p, q, n\}$. We have picked $a < n$, so if $gcd(a, n) > 1$, it has to be $\in \{p, q\}$ and we are done.
3. Otherwise, check for each $i = 0, ..., s-1$ if $gcd((a^k)^{2^i} - 1, n) \neq \{1, n\}$. If so, we have found a factor of n and can exit.

Amazingly, the success probability for each iteration of this procedure is $\frac{1}{2}$! How come? We begin with the following:

$$\begin{aligned} gcd(a, n) = 1 &\implies (a^k)^{2^s} = a^{x \cdot \phi(n)} = (a^{\phi(n)})^x \equiv 1 \mod n \\ &\implies (a^k)^{2^s} - 1 \equiv 0 \mod n \\ &\implies gcd((a^k)^{2^s} - 1, n) = n \end{aligned}$$

We have here used Fermat's Little Theorem. This congruence also holds modulo p and q, ns co-prime factors (by the Chinese Remainder Theorem, I think). Now, enter group theory. In RSA, we operate in $\mathbb{Z}_n^*$, where the asterisk means we are only interested in elements that have a multiplicative inverse. By CRT, $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

$\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$ are subgroups of $\mathbb{Z}_n^*$. We know that the order of a^k, $o(a^k)$, defined as $(a^k)^{o(a^k)} \equiv 1$, is equal to 2^s in $\mathbb{Z}_n^*$. In $\mathbb{Z}_p^*$, $\mathbb{Z}_q^*$, the order of a^k may be smaller (or for sure is?). Luckily, by Lagrange's theorem, the order of a^k in either of the two subgroups has to divide its order in $\mathbb{Z}_n^*$.

Let g, h be generators of $\mathbb{Z}_p^*$, $\mathbb{Z}_q^*$ respectively. Then $a^k \cong (g^y, h^z)$ in $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Let $o(g^y) = 2^{l_1}$ and $o(h^z) = 2^{l2}$. If $l_1 \neq l_2$, we have a success. Assume without loss of generality $l_1 < l_2$, then

$$\begin{aligned} (a^k)^{2^{l_1}} &\equiv 1 \mod p \\ (a^k)^{2^{l_2}} &\equiv j \mod q, j \neq 1 \\ p &| (a^k)^{2^{l_1}} - 1 \\ q \nmid p &| (a^k)^{2^{l_1}} - 1 \\ \implies gcd((a^k)^{2^{l_1}} &- 1, n) = p \end{aligned}$$