ANTA20250512

May 12, 2025

Common modulus attack

Suppose that at a company it is decided that they will use the RSA cryptosystem with a given modulus N and each employee will have a personalized public encryption exponent e and corresponding private decryption exponent d. A manager sends the same message m to two of his/her colleagues. It will yield two different ciphertexts

$$\begin{aligned} c_1 &\equiv m^{e_1} \pmod N, \\ c_2 &\equiv m^{e_2} \pmod N. \end{aligned}$$

Here N, e_1, e_2, c_1 and c_2 are all known and one can read the secret message without knowing one of the private keys d_1, d_2. The approach is based on the extended Euclidean algorithm. We compute s and t for which

$$se_1 + te_2 = 1.$$

The above system of congruences provide that

$$\begin{aligned} c_1^s &\equiv (m^{e_1})^s \pmod N, \\ c_2^t &\equiv (m^{e_2})^t \pmod N. \end{aligned}$$

It follows that

$$c_1^s c_2^t \equiv m^{se_1+te_2} \equiv m \pmod N.$$

[2]:

```
def RSAcommon(m,e1,e2,N):
    c1=(m^e1)%N
    c2=(m^e2)%N
    pretty_print(html('The first ciphertext is %s'%latex(c1)))
    pretty_print(html('The second ciphertext is %s'%latex(c2)))
    g,s,t=xgcd(e1,e2)
    pretty_print(html('We have $s=%s$ and $t=%s$'%(latex(s),latex(t))))
    M=(c1^s*c2^t)%N
    pretty_print(html('The message is %s'%latex(M)))
    return M
RSAcommon(500,17,5,1591)
```

```
The first ciphertext is 849

The second ciphertext is 22

We have \(s=-2\) and \(t=7\)

The message is 500
```

```
[2]: 500
```

Low public exponent attack

In the RSA cryptosystem the encryption process might be quite costly if the public exponent e is large. It may be a problem in terms of time and battery power on some limited devices like smart cards. In these cases one might choose a small public exponent like $e = 3$. Suppose that Alice is going to send the same message to Bob, Chris and David, say m. She knows the public keys of Bob, Chris and David, let us denote these by N_B, N_C and N_D. Alice computes the ciphertexts as follows

$$\begin{aligned} c_B &\equiv m^3 \pmod{N_B}, \\ c_C &\equiv m^3 \pmod{N_C}, \\ c_D &\equiv m^3 \pmod{N_D}. \end{aligned}$$

Assume that Eve, an eavesdropper, obtains these ciphertexts. Let us see how to recover m. If N_B, N_C and N_D are not pairwise relatively prime numbers, then Eve can factor at least two of them and easily computes the private keys. So we may assume that those numbers are pairwise relatively prime. In this case Eve applies the Chinese Remainder Theorem to determine c for which $c \equiv m^3 \pmod{N_B N_C N_D}$. Since m is less than N_B, N_C and N_D, we get that $m^3 < N_B N_C N_D$. Thus instead of a congruence we have equality over the integers, that is $c = m^3$. Taking the cubic root of c over the integers yields the message m.

```
[1]: def LowExponent(NB,NC,ND,m):
         pretty_print(html('The message is %s'%latex(m)))
         cB=(m^3)%NB
         cC=(m^3)%NC
         cD=(m^3)%ND
         pretty_print(html('Bob receives: %s'%latex(cB)))
         pretty_print(html('Chris receives: %s'%latex(cC)))
         pretty_print(html('David receives: %s'%latex(cD)))
         M3=CRT_list([cB,cC,cD], [NB,NC,ND])
         M=(M3)^(1/3)
         pretty_print(html('The attacker obtains: %s'%latex(M)))
         return M
     LowExponent(2257,2581,4223,123)
```

```
The message is 123

Bob receives: 1099

Chris receives: 2547

David receives: 2747

The attacker obtains: 123
```

```
[1]: 123
```

The equation $ax^2 + by^2 = z^2$

Lemma 5. *Suppose $a, b, b', e \in \mathbb{Z}$ are such that $a + bb'e^2$ is a square and $bb'e^2 \neq 0$. Then $Z^2 = aX^2 + bY^2$ has a non-trivial $\mathbb{Q}$-solution if and only if $Z^2 = aX^2 + b'Y^2$ does.*

Proof. By symmetry, it suffices to prove one direction of the biconditional. Suppose (x_0, y_0, z_0) is a non-trivial $\mathbb{Q}$-solution to $Z^2 = aX^2 + bY^2$. So

$$by_0^2 = z_0^2 - ax_0^2 = \big(z_0 + x_0\sqrt{a}\,\big)\big(z_0 - x_0\sqrt{a}\,\big)$$

(for a fixed choice of square root $\sqrt{a} \in \mathbb{C}$).

Now write $a + bb'e^2 = u^2$. So

$$bb'e^2 = u^2 - a = \big(u + \sqrt{a}\big)\big(u - \sqrt{a}\big).$$

Combining we get

$$\begin{aligned}
b'(bey_0)^2 &= (bb'e^2)(by_0^2) \\
&= \big(u + \sqrt{a}\big)\big(u - \sqrt{a}\big)\big(z_0 + x_0\sqrt{a}\big)\big(z_0 - x_0\sqrt{a}\big) \\
&= \big(u + \sqrt{a}\big)\big(z_0 + x_0\sqrt{a}\big)\big(u - \sqrt{a}\big)\big(z_0 - x_0\sqrt{a}\big) \\
&= \Big((uz_0 + ax_0) + (ux_0 + z_0)\sqrt{a}\Big)\Big((uz_0 + ax_0) - (ux_0 + z_0)\sqrt{a}\Big) \\
&= (uz_0 + ax_0)^2 - a(ux_0 + z_0)^2.
\end{aligned}$$

So $(ux_0 + z_0,\ bey_0,\ uz_0 + ax_0)$ is a $\mathbb{Q}$-solution to $Z^2 = aX^2 + b'Y^2$. Since

$$\begin{bmatrix} u & 0 & 1 \\ 0 & be & 0 \\ a & 0 & u \end{bmatrix}$$

has determinant $be(u^2 - a) = be(bb'e^2) \neq 0$, the above solution to $Z^2 = aX^2 + b'Y^2$ is non-trivial. □

Theorem 1. *Suppose that $a, b \in \mathbb{Z}$ are integers such that (a, b) satisfies the descent condition. Then $Z^2 = aX^2 + bY^2$ has a non-trivial $\mathbb{Z}$-solution.*

Proof. Observe that if $a = 1$ then $(1, 1, 0)$ is a non-trivial solution, and if $b = 1$ then $(1, 0, 1)$ is a non-trivial solution. Our goal is to use descent until we get to an equation with $a = 1$ or $b = 1$.

For convenience, suppose that $|a| \leq |b|$. If $|a| = |b| = 1$ we are done since either a or b must be positive. So assume that $|b| \geq 2$.

Since (a, b) satisfies the descent condition, a is a square modulo $|b|$. Let u be an integer of smallest absolute value so that $a \equiv u^2 \bmod |b|$. In other words, $|u| \leq |b|/2$, and b divides $u^2 - a$. Write $u^2 - a = bb'e^2$ where b' is square free.

If $bb'e^2 = 0$, then a is a square. Since a is square free, $a = 1$ and we are done. So from now on assume that b' and e are non-zero.

Claim: $|b'| < |b|$. To see this observe that

$$|b||b'||e^2| = |u^2 - a| \le |u|^2 + |a| \le |b|^2/4 + |b|, \qquad \text{so} \qquad |b'| \le |b|/4 + 1.$$

This gives

$$|b'| \le |b|/4 + 1 < |b|/4 + 3|b|/4 = |b|.$$

($1 < 3|b|/4$ since we are in the case where $|b| \ge 2$.) By Lemma 5 we have reduced the equation to one with smaller coefficients (their product is smaller in absolute value).

The new equation has coefficients a and b'. These coefficients satisfy the descent condition by the previous lemma. If either is 1 we are done. Otherwise repeat the descent, reducing the problem to an equation with yet smaller coefficients. In this way we continue until one of the coefficients is 1 and we are guaranteed a solution. □

[ ]: