TIPE : Draft

Contents

1 Common modulus

Given : N (common modulus), e, d (known public and private exponent), e_1 (public exponent linked to searched private one).
First search $p, q \in \mathbb{P} \mid N = pq$.
We have

$$ed \equiv 1 \ [\phi(N)]$$
$$\gcd(e, \phi(N)) = 1$$

Let $k = ed - 1$. By definition, $\exists \lambda \in \mathbb{N} \mid ed - 1 = \lambda \cdot \phi(N)$.
However $\phi(N) = (p-1)(q-1)$, so $2^2 \mid \phi(N)$ (because $p, q \in \mathbb{P}$, thus $p \equiv q \equiv 1 \ [2]$)

Let $n = pq$, and $x \in \mathbb{Z}/n\mathbb{Z}$.

$$\begin{aligned} x \in (\mathbb{Z}/n\mathbb{Z})^* \quad & \Leftrightarrow \quad \exists y \in \mathbb{Z}/n\mathbb{Z} \mid xy \equiv 1 \ [n] \\ & \Leftrightarrow \quad \exists (y, k) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{N} \mid xy - kn = 1 \\ & \Leftrightarrow \quad \gcd(x, n) = 1 \end{aligned}$$

2 Fermat factorisation

if n is composite,

$$\exists a, b \in \mathbb{N} \mid n = a^2 - b^2 = (a-b)(a+b) = pq \quad (*)$$

So we have $b^2 = a^2 - n$.
Then choose $a = \lceil \sqrt{n} \ \rceil$. If $a^2 - n$ is a square, won. Otherwise, increment a.

Proof for $(*)$:
If $n = pq$, then we have :

$$\left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = \frac{p^2 + 2pq + q^2}{4} - \frac{p^2 - 2pq + q^2}{4} = pq = n \ \blacksquare$$

3 Same message

3.1 same modulus

If the same message m is sent to Alice (e_1, n) and Bob (e_2, n).
Alice receives $c_1 = m^{e_1} \mod n$
Bob receives $c_2 = m^{e_2} \mod n$.
We have :

$$c_1 c_2 \equiv m^{e_1} m^{e_2} \equiv m^{e_1 + e_2} \ [n]$$

(pointless)
If $\gcd(e_1, e_2) = 1$,

$$\exists a, b \in \mathbb{Z} \mid ae_1 + be_2 = 1$$

and

$$c_1^a \cdot c_2^b \equiv m^{a \cdot e_1} \cdot m^{b \cdot e_2} \equiv m^{ae_1 + be_2} \equiv m \ [n]$$

But not a realistic situation : Alice ans Bob can calculate each other's private exponent.

3.2 same message

From https://security.stackexchange.com/questions/166370/how-to-do-rsa-same-message-attack
Let be m the message, and $\forall i \in [\![1 \ ; \ 3]\!]$, n_i the modulus.
The keys are (e, n_i), where $e = 3$.
The encrypted messages are :

$$\forall i \in [\![1 \ ; \ 3]\!], \ c_i \equiv m^e \ [n_i]$$

We have the following system (we need e equations in fact) :

$$\begin{cases} c_1 \equiv m^e \ [n_1] \\ c_2 \equiv m^e \ [n_2] \\ c_3 \equiv m^e \ [n_3] \end{cases}$$

CRT (why ?)

$$M = \prod_{k=1}^{e} n_k$$

$$\forall k \in [\![1 \ ; \ e]\!], \ M_k = \frac{M}{n_k}$$

$$m^3 \equiv \left(\sum_{k=1}^{e} c_k \cdot M_k \cdot (M_k^{-1} \mod m_i) \right) \mod M$$

4 Large numbers

4.1 Large message

Let m be a message, $c = m^e \ [N]$.
If m is close of N (*cf* paper on large private exponent)
We have

$$N - N^{\frac{1}{e}} < m < N \quad \Leftrightarrow \quad 0 < \underbrace{N - m}_{m_0} < N^{\frac{1}{e}}$$

$$\Leftrightarrow \quad 0 < {m_0}^e < N$$

So if $N - N^{\frac{1}{e}} < m < N$, let $m_0 = N - m$, and we have

$$m_0 \equiv N - m \equiv -m\ [N]$$

So as $e \equiv 1\ [2]$,

$$m_0^e \equiv (-m)^e \equiv (-1)^e m^e \equiv -m^e \equiv -c\ [N]$$

Thus we can calculate m_0 :

$$m_0 = (-c \mod N)^{\frac{1}{e}}$$

And we can recover m :

$$m = N - m_0 = N - (-c \mod N)^{\frac{1}{e}}$$

5 Hastad Attack

5.1 Notations

Let m be the message, p the number of messages, $(e_k)_{k\in[\![1\ ;\ p]\!]}$ the public exponents, and $(n_k)_{k\in[\![1\ ;\ p]\!]}$ the modulus.
Let $(c_k)_{k\in[\![1\ ;\ p]\!]}$ the corresponding cipher texts. We have :

$$\begin{cases} c_1 & \equiv & m^{e_1}\ [n_1] \\ & \vdots & \\ c_k & \equiv & m^{e_k}\ [n_k] \\ & \vdots & \\ c_p & \equiv & m^{e_p}\ [n_p] \end{cases}$$

We suppose that

$$\forall (i,j) \in [\![1\ ;\ p]\!]^2,\ i \neq j \Rightarrow n_i \wedge n_j = 1$$

Otherwise, one can factor the modulus by calculating the gcds.

5.2 CRT

> CRT :
> Let $n \in \mathbb{N} \mid n \geqslant 2$, and $(a_k)_{k\in[\![1\ ;\ n]\!]} \subset \mathbb{N}^* \setminus \{1\}$ such that
>
> $$\forall (i,j) \in [\![1\ ;\ n]\!]^2,\ i \neq j \Rightarrow a_i \wedge a_j = 1$$
>
> Then, with $a = \prod_{k=1}^{n} a_k$:
>
> $$\begin{array}{rcccl} \varphi & : & \mathbb{Z}/a\mathbb{Z} & \longrightarrow & \prod_{k=1}^{n} \mathbb{Z}/a_k\mathbb{Z} \\ & & cl_a(k) & \longmapsto & (cl_{a_1}(k), \ldots, cl_{a_n}(k)) \end{array}$$

is a bijection (even a ring isomorphism).

Determination of φ^{-1} :

$$\begin{aligned}
& \varphi^{-1}((cl_{a_1}(\alpha_1), \dots, cl_{a_n}(\alpha_n))) \\
= \; & \varphi^{-1}\left(\sum_{k=1}^{n} \alpha_k \left(cl_{a_1}(0), \dots, cl_{a_{k-1}}(0), cl_{a_k}(1), cl_{a_{k+1}}(0), \dots, cl_{a_n}(0)\right)\right) \\
= \; & \sum_{k=1}^{n} \alpha_k \underbrace{\varphi^{-1}\left(cl_{a_1}(0), \dots, cl_{a_{k-1}}(0), cl_{a_k}(1), cl_{a_{k+1}}(0), \dots, cl_{a_n}(0)\right)}_{cl_a(m_k)} \\
= \; & \sum_{k=0}^{n} \alpha_k cl_a(m_k)
\end{aligned}$$

Is is enough to find suitable m_k, *i.e* such that $\forall k \in [\![1 \; ; \; n]\!]$,

$$\begin{cases} m_k \in \mathbb{Z} \\ \forall i \in [\![1 \; ; \; n]\!] \setminus \{k\}, \; m_k \equiv 0 \; [a_i] \\ m_k \equiv 1 \; [a_k] \end{cases}$$

Let $A = \prod_{k=1}^{n} a_k$, and $\forall k \in [\![1 \; ; \; n]\!]$, $A_k = \dfrac{A}{a_k}$

As the a_k are pairwise coprime, $\forall k \in [\![1 \; ; \; n]\!]$, $A_k \wedge a_k = 1$, so using BÉZOUT's identity :

$$\exists B_k, b_k \in \mathbb{Z} \mid A_k B_k + a_k b_k = 1$$

$(B_k \equiv (A_k)^{-1} \;\; [a_k])$

Let $\forall k \in [\![1 \; ; \; n]\!]$, $m_k = A_k B_k \in \mathbb{Z}$.

We have, $\forall k \in [\![1 \; ; \; n]\!]$:

$$m_k \equiv A_k B_k \equiv 1 - a_k b_k \equiv 1 \; [a_k]$$

and $\forall i \in [\![1 \; ; \; n]\!] \setminus \{k\}$:

$$m_k \equiv A_k B_k \equiv 0 \; [a_i]$$

because $a_i | A_k$.

And finally :

$$\varphi^{-1}\left(cl_{a_1}(\alpha_1), \dots, cl_{a_n}(\alpha_n)\right) = \sum_{k=1}^{n} \alpha_k cl_a(A_k B_k)$$

So applied here :

Suppose that all e_k are equal to $e \in \mathbb{Z}$.

Then by the previous thing, there is one solution to the system, which is :

$$m^e \equiv \sum_{k=1}^{p} c_k N_k M_k \; [N]$$

where $\forall k \in [\![1 ; p]\!]$:

$$\begin{aligned} N &= \prod_{i=1}^{p} n_i \\ N_k &= \prod_{\substack{i=1 \\ i \neq k}}^{p} n_i = \frac{N}{n_k} \\ M_k &\equiv (N_k)^{-1} \ [n_k] \end{aligned}$$

Then we can recover m by calculating the e^{th} root of m^e (if $m^e < N$).

5.3 Number of equations needed

• Finding the minimal number of equations needed :

If we suppose that all moduli are of the same size (approximatively the same number of bits), we have :

$$m^e < N \Rightarrow m < \sqrt[e]{N} = \prod_{k=1}^{p} \sqrt[e]{n_k} \approx \sqrt[e]{n_1}^p = n_1{}^{\frac{p}{e}}$$

So if $p < e$, then $\frac{p}{e} < 1$, and $n_1{}^{\frac{p}{e}} < n_1$.

But messages can be up to n_1 long, so we need to have $p \leqslant e$.

—

Example with $e = 3$: if we have only two equations, then if

$$m \geqslant n^{\frac{2}{3}} = \frac{n}{\sqrt[3]{n}}$$

then we won't be able to compute the e^{th}.

—

Let note s the bit size of the modulus (often 2048), so $n_1 \approx 2^s = n$.

With a message m, the minimum number of equations p that are needed is such that :

$$\begin{aligned} & m < (2^s)^{\frac{p}{e}} = 2^{\frac{sp}{e}} \\ \Leftrightarrow \quad & \frac{sp}{e} > \log_2(m) \\ \Leftrightarrow \quad & \boxed{p > \frac{e}{s} \log_2(m)} \end{aligned}$$

Typically, $e = 2^{16} + 1$, $s = 2048$, so $\frac{e}{s} = \frac{2^{16}+1}{2^{11}} \approx \frac{2^{16}}{2^{11}} = 2^5 = 32 \approx \frac{e}{s}$. The number m is the encoded version of the string m_s. If m_s is l characters long, then $\boxed{\log_2(m) \approx \alpha l}$, where $\alpha = 8$.

So in order for the attack to work, we need $p > 256l$ in this case. This is thus not really realistic ...

We have also $p > \alpha \frac{e}{s} l$.

If we have p equations, it is possible to recover the message if that one has less than $\frac{ps}{\alpha e}$ char.

With $p = 3$, $e = 3$, $s = 2048$, then if $l < 2^{11-3} = 256$, we are able to recover m.

5.4 Trying with large messages

- If $M - M^{\frac{1}{e}} < m < M$, with $M \approx n^p$, at the first approximation, $m \approx M$, then

$$\frac{e}{s}\log_2(m) \approx \frac{e}{s}\log_2(n^p) = \frac{e}{s}ps = ep$$

so we need e times more equations by using the normal way (maybe a bit less because of the approximation).

We can calculate, with the CRT (Hastad attack), m^e $[M]$, and then we can recover m using 4.1.

> So if we are in the right conditions, and if we need to use ep equations to recover m using the first method, then we will be able to recover m with only p equations using this method.

We have $p = \left\lceil \frac{e}{s}\log_2(m) \right\rceil$. If $\exists p' \in \mathbb{N} \mid p = ep'$, we can recover m with only p' equations. Is it possible if we have more than p' equations ? Does this gives a constraint on the message ?

Is it possible to do something with $m' = M - m$? With the thing below, we have $\log_2(M) \approx \log_2(m)$, so $m' \approx 0$ (need to go to the next order ?). In fact, we have $0 < m' < M^{\frac{1}{e}}$.

If we have m', we can calculate $p' = \left\lceil \frac{e}{s}\log_2(m') \right\rceil$. Then let $p = ep'$, and let m such that $p = \left\lceil \frac{e}{s}\log_2(m) \right\rceil$.

We now need to find M such that $m' = M - m$.

But M depends on p !

—

If we have m and p, is it possible to make m' ? We need $\frac{p}{e}$ equations, but this should be an int. What if it is not ?

But we did things the opposite way : in reality we have the message encrypted, we don't know its original length, and we have a certain number of equations.

However, given a message, can we determine the number of equations needed to recover it using this method ?

In order for this method to work, we need to have $p \in \mathbb{N}^*$ such that

$$n^p - n^{\frac{p}{e}} < m < n^p$$

$i.e$ such that

$$2^{sp} - 2^{\frac{sp}{e}} < m < 2^{sp} \quad \Leftrightarrow \quad n^p\left(1 - n^{p\frac{1-e}{e}}\right) < m < n^p$$
$$\Leftrightarrow$$

What does it implies on p ?

—

If $M - M^{\frac{1}{e}} < m < M$, and $\log_2(m) \approx \alpha l$, where l is the length of the message (not encoded), α depends on the encoding, then

$$\log_2\left(M - M^{\frac{1}{e}}\right) < \alpha l < \log_2(M) = sp$$

And $M - M^{\frac{1}{e}} = 2^{sp} - 2^{\frac{sp}{e}} = 2^{sp}\left(1 - 2^{sp\frac{1-e}{e}}\right)$ so

$$\frac{sp + \log_2\left(1 - 2^{sp\frac{1-e}{e}}\right)}{\alpha} \leqslant l \leqslant \frac{sp}{\alpha}$$

But as $e \geqslant 3$, we have $-1 \leqslant \dfrac{1-e}{e} \leqslant -\dfrac{2}{3}$, so as $sp \gg 1$ ($s = 2048$, $p \in \mathbb{N}^*$),

$$\varepsilon = 2^{sp\frac{1-e}{e}} \approx 0$$

and

$$\frac{sp}{\alpha} \leqslant l \leqslant \frac{sp}{\alpha}$$

So $l = \dfrac{sp}{\alpha}$. As $l \in \mathbb{N}$, this is only possible if

$$\alpha \mid sp$$

—

At least, we need to have $sp + \varepsilon \leqslant \log_2(m) \leqslant sp$, $i.e$ $\boxed{\log_2(m) \approx sp = \log_2(M)}$.

6 Wiener's attack

6.1 Classic attack

Let $\left|\begin{array}{l} p, q \in \mathbb{P} \mid q < p < 2q \\ n = pq \\ d \in \left[1\ ;\ \frac{1}{3}n^{\frac{1}{4}}\right[\cap \mathbb{N} \\ e \in [\![1\ ;\ \phi(n)]\!] \mid ed \equiv 1\ [\phi(n)] \end{array}\right.$. Let be $\varphi = \phi(n)$.

Given (e, n), one can efficiently recover d.

Proof :

Since $ed \equiv 1\ [\varphi]$, $\exists k \in \mathbb{N} \mid ed - k\varphi = 1$, so :

$$\begin{aligned} & \frac{ed - k\varphi}{d\varphi} = \frac{1}{d\varphi} \\ \Rightarrow \quad & \frac{e}{\varphi} - \frac{k}{d} = \frac{1}{d\varphi} \\ \Rightarrow \quad & \left|\frac{e}{\varphi} - \frac{k}{d}\right| = \frac{1}{d\varphi} \end{aligned}$$

Hence $\frac{k}{d}$ is an approximation of $\frac{e}{\varphi}$.

We can now try to approximate φ with n :

$$\varphi = \phi(n) = (p-1)(q-1) = n - p - q + 1$$

And $p + q - 1 < 3\sqrt{n}$: since $\begin{cases} p < 2q \\ q < p \end{cases}$ (by hypothesis), we have

$$\begin{cases} p + q < 3q \\ q^2 < pq = n \end{cases} \Rightarrow \begin{cases} p + q < 3q \\ q < \sqrt{n} \end{cases} \Rightarrow p + q < 3\sqrt{n} \Rightarrow p + q - 1 < 3\sqrt{n}$$

So $|n - \varphi| = |p + q - 1| < 3\sqrt{n}$.

Then we have :

$$\begin{aligned} \left|\frac{e}{n} - \frac{k}{d}\right| &= \left|\frac{ed - nk}{nd}\right| \\ &= \left|\frac{ed - k\varphi + k\varphi - nk}{nd}\right| \\ &= \left|\frac{1 - k(n - \varphi)}{nd}\right| \\ &< \frac{1 + |k(n - \varphi)|}{|nd|} \\ &\leqslant \left|\frac{k(n - \varphi)}{nd}\right| \\ &\leqslant \left|\frac{3k\sqrt{n}}{nd}\right| \\ &= \frac{3k}{d\sqrt{n}}. \end{aligned}$$

Then, $k\varphi = ed - 1 < ed$ and $e < \varphi$, so $k < \frac{e}{\varphi} d < d$, so :

$$k < d < \tfrac{1}{3} n^{\frac{1}{4}} \Rightarrow \frac{k}{d} < 1 < \frac{n^{\frac{1}{4}}}{3d}$$

Hence :

$$\begin{aligned} \left|\frac{e}{n} - \frac{k}{d}\right| &\leqslant \frac{k}{d}\frac{3}{\sqrt{n}} \\ &\leqslant \frac{n^{\frac{1}{4}}}{3d}\frac{3}{\sqrt{n}} \\ &= \frac{1}{dn^{\frac{1}{4}}} \end{aligned}$$

And :

$$2d^2 < \frac{2}{3}dn^{\frac{1}{4}} < dn^{\frac{1}{4}} \Rightarrow \frac{3}{2dn^{\frac{1}{4}}} < \frac{1}{2d^2}$$

Hence :

$$\boxed{\left|\frac{e}{n} - \frac{k}{d}\right| \leqslant \frac{1}{dn^{\frac{1}{4}}} \leqslant \frac{1}{2d^2}}$$

So $\frac{e}{n}$ is an approximation of $\frac{k}{d}$. In fact, all fraction approximating $\frac{e}{n}$ can be obtained as the convergents of the continued fraction expansion of $\frac{e}{n}$.

The number of such fractions is bounded by $\log_2(n)$ (Why ???), and $\frac{k}{d}$ is one of them.

Let k_i and d_i the numerator and denominator of the i-th convergent of the expansion of $\frac{e}{n}$ ($i \in [\![0 \ ; \ i_{\mathrm{m}}]\!]$).

Now compute, $\forall i \in [\![0 \ ; \ i_{\mathrm{m}}]\!]$, $\varphi_i = \dfrac{e \cdot d_i - 1}{k_i}$.

We know that :

$$\begin{aligned} &\begin{cases} n = pq \\ \varphi = (p-1)(q-1) \end{cases} \\ \Rightarrow \ &\begin{cases} n = pq \\ \varphi = n - p - q + 1 \end{cases} \\ \Rightarrow \ &\begin{cases} pq = n \\ p + q = n - \varphi + 1 \end{cases} \\ \Rightarrow \ & p, q \in \{x \in \mathbb{R} \mid x^2 - (n - \varphi + 1)x + n = 0\} \end{aligned}$$

($p \neq q$, otherwise factoring n is simple ...)

So we can calculate $\forall i \in [\![0 \ ; \ i_{\mathrm{m}}]\!]$ the roots of $x^2 - (n - \varphi_i + 1)x + n$, and check if they factor n.

6.2 Extension with large private exponent

We use the same notations as above, but we take d satisfying :

$$\sqrt{6}(\varphi - d) < n^{\frac{1}{4}}$$

so

$$\begin{aligned}\sqrt{6}(\varphi - d) < n^{\frac{1}{4}} \quad &\Leftrightarrow \quad \sqrt{6}d > \sqrt{6}\varphi - n^{\frac{1}{4}} \\ &\Leftrightarrow \quad d > \varphi - \frac{\sqrt{6}}{6}n^{\frac{1}{4}}\end{aligned}$$

So $d \in \left]\varphi - \frac{\sqrt{6}}{6}n^{\frac{1}{4}}\ ;\ \varphi\right[$.

$$\begin{aligned}\varphi - \frac{\sqrt{6}}{6}n^{\frac{1}{4}} < d < \varphi \quad &\Leftrightarrow \quad -\varphi < -d < \frac{\sqrt{6}}{6}n^{\frac{1}{4}} - \varphi \\ &\Leftrightarrow \quad 0 < \varphi - d < \frac{\sqrt{6}}{6}n^{\frac{1}{4}}\end{aligned}$$

So let $D = \varphi - d$.

We have $D < \frac{1}{\sqrt{6}}n^{\frac{1}{4}}$

The above proof is still correct for such a D (because $\frac{\sqrt{2}}{2} < 1$)