Attacks on RSA

Low exponent attack

$\mathcal{E}(m) = m^e \mod n$ $\quad$ ((n,e) is the public key)

$\mathcal{D}(c) = c^d \mod n$ where $de \equiv 1 \mod \phi(n)$

Three people B, C & D receive message from A.
e (the exponent) is the same but n_B, n_C & n_D
are values of n (resply)

B, C & D receive $\underline{c_B = m^e \mod n_B}$,
$c_C = m^e \mod n_C$
$c_D = m^e \mod n_D$
respectively.

Case 1 $\quad$ ~~$\gcd(n_B, n_C, n_D) = 1$~~ $\quad$ $\left.\begin{array}{l}\gcd(n_B, n_C) = 1 \\ \gcd(n_C, n_D) = 1 \\ \gcd(c_B, n_D) = 1\end{array}\right\}$

(pair-wise coprime)
set $N = n_B n_C n_D$

Chinese remainder theorem $\exists\ x \in \mathbb{Z}_N$

s.t. $\left.\begin{array}{l} x \equiv c_B \mod n_B \\ x \equiv c_C \mod n_C \\ x \equiv c_D \mod n_D. \end{array}\right\}$

$$\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}_{n_B} \times \mathbb{Z}_{n_C} \times \mathbb{Z}_{n_D}$$
$$x \longmapsto (c_B, c_C, c_D)$$
$$t \longmapsto (\bar{t}, \bar{\bar{t}}, \bar{\bar{\bar{t}}})$$

$\ker \psi = \langle n_B n_C n_D \rangle = \langle N \rangle$

$0 \leq x \leq N-1 = n_B n_C n_D - 1$

$m \leq n_B, n_C, n_D.$

If $e=3$ ~~$e \leq 3$~~, then
$m^3 \leq n_B n_C n_D - 1$, so $x = m^3$
you have

m as ~~$\sqrt[3]{m^3}$~~ $\sqrt[3]{x}$ in $\mathbb{Z}_N$

$\mathbb{Z}_N \cong \mathbb{Z}_{n_B} \times \mathbb{Z}_{n_C} \times \mathbb{Z}_{n_D}$

$\tilde{t} \mapsto (\bar{t}, \bar{\bar{t}}, \bar{\bar{\bar{t}}})$

$(x \bmod N) \mapsto (x \bmod n_B, x \bmod n_C, x \bmod n_D)$

~~We need to~~

Attacker needs to ~~ob~~ observe

cipher text of e recievers

(we have discussed the case of $e=3$)

More generally for $n_1, n_2, \ldots, n_e$ pairwise coprime

get $c_i \equiv m^e \bmod n_i$

Then by CRT get x as $x \equiv c_i \bmod n_i$ $(x \in \mathbb{Z}_{n_1 n_2 \cdots n_e})$

Then $\underline{\sqrt[e]{x} = m}$ $\qquad \underline{m^e \leq n_1 n_2 \cdots n_e - 1}$

$c_i \equiv m^3 \bmod n_i$ $\qquad \underline{i = 1, 2, 3}$

$\exists\, x \equiv m^3 \bmod n_i$ $\qquad i = 1, 2, 3.$

$x \equiv m^3 \bmod n_1 n_2 n_3$ $\qquad (n_i \mid x - m^3 \Rightarrow n_1 n_2 n_3 \mid x - m^3)$

$\boxed{x = m^3}$ because $m < n_i \Rightarrow m^3 < n_1 n_2 n_3$

Find $m = \sqrt[3]{x}$ in $\mathbb{Z}$

$[r] = [s]$ in $\mathbb{Z}_N$

if ~~iff~~ & only if $r = s$ for

$\underline{0 \leq r, s \leq N-1}$

~~If n_1, n_2, n_3 are not pairwise coprime~~

~~then take $N = LCM(n_1, n_2, n_3)$ & try to attack~~

Extended div alg. to find GCD & get a prime factor &

then find the structure!

---

(2). $\underline{n \text{ is common;}}$ $\qquad$ reciever suggest e

(& keep d with $de = 1 \bmod \phi(n)$)

$B_1 = B \longrightarrow (n, e_1)$

$B_2 = C \longrightarrow (n, e_2)$

$B_3 = D \longrightarrow (n, e_3)$

$\mathcal{E}_i(m) \equiv m^{e_i} \mod n = c_i$ recieved by B_i

Assume $\gcd(e_1, e_2, e_3) = 1$

Then find x_i s.t. $\sum x_i e_i = 1$

$$\prod_{i=1}^{3} C_i^{x_i} = \prod_{i=1}^{3} (m^{e_i})^{x_i} = m^{\sum_{i=1}^{3} e_i x_i} = m$$

---

(3)

$$A \xrightarrow[m \longmapsto \mathcal{E}(m)]{\overset{E}{\downarrow}} B$$

(n, e) public $\quad s^e c \longmapsto m'$ $\qquad c = m^e \; (\mathcal{E}(m)) \pmod n$

E = Attacker picks s & apply $s^e \cdot c \pmod n$

E = Attacker sends $s^e \cdot c$ to B

B decrypts $s^e c$: $m' = \mathcal{D}(s^e c) = (s^e c)^d$
$= s\, m$

E get to know somehow $m' = s m$.

He gets $m = s^{-1} m' \pmod n$

Strong prime: A prime p is called strong if

1. $p-1$ has a large prime factor r
2. $r-1$ has a large prime factor t
3. $p+1$ has a large prime factor s

Observe, $p = kr + 1$, k is even. so write $p = 2jr + 1$

$r = k't + 1$, k' is even so $r = 2lt + 1$

$p = k''s - 1$, k'' is even so $\underline{p = 2ms - 1}$

$$p = 2j(2lt+1) + 1$$

Choose large primes r, s & t & then for various j, l & m find p so that p is a prime.