2.5 Iteration Attack

Consider a bijective map $E\colon M \longrightarrow M$ of a finite set M onto itself and its inverse $D = E^{-1}$ (think of E as an encryption function). Then E is an element of the full symmetric group $\mathfrak{S}(M)$ that has the (huge) order $\#\mathfrak{S}(M) = (\#M)!$. Nevertheless this group is finite, thus there is an $s \in \mathbb{N}_1$ with $E^s = \mathbf{1}_M$, hence

$$D = E^{s-1}.$$

As a consequence an attacker can compute D from E by sufficiently many iterations. This attack is relevant only for asymmetric ciphers where the attacker knows E. The only protection against it is *to choose the order of E, the smallest $s \geq 1$ with $E^s = \mathbf{1}_M$, as large as possible.*

The Example of RSA

Let $M = \mathbb{Z}/n\mathbb{Z}$, then $\#\mathfrak{S}(M) = n!$, where n itself is a very large integer. The attacker could compute $E^{n!-1}$, but even the fastest power algorithm is not fast enough to accomplish this task in this universe. So the attack doesn't seem to put RSA into immediate danger.

However, as a closer look reveals, RSA encryption functions are contained in a significantly smaller subgroup of $\mathfrak{S}(M)$—fortunately the attacker doesn't know its order. To see this consider the map

$$\Phi\colon \mathbb{N} \longrightarrow \operatorname{map}(M, M), \quad e \mapsto E_e \quad \text{with } E_e(a) = a^e \bmod n.$$

Here are some of its properties:

1. For $e, f \in \mathbb{N}$ we have $E_{ef} = E_e \circ E_f$ since $a^{ef} \equiv (a^f)^e \pmod{n}$ for all $a \in M$. Hence Φ is a homomorphism of the multiplicative semigroup $\mathbb{N}$.

2. If $e \equiv f \pmod{\lambda(n)}$, then $E_e = E_f$: Assume $f = e + k\lambda(n)$, then $a^f = a^{e+k\lambda(n)} \equiv a^e \pmod{n}$ for all $a \in M$.

3. If $e \bmod \lambda(n)$ is invertible, then E_e is bijective: Assume $de \equiv 1 \pmod{\lambda(n)}$, then $E_d \circ E_e = E_1 = \mathbf{1}_M$. Hence the map

   $$\bar{\Phi}\colon \mathbb{M}_{\lambda(n)} \longrightarrow \mathfrak{S}(M)$$

   induced by Φ is a group homomorphism.

4. $\bar{\Phi}$ is injective: For if $\Phi(e) = E_e = \mathbf{1}_M$, then $a^e \equiv a \pmod{n}$ for all $a \in M$, hence $a^{e-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{M}_n$, hence $\lambda(n) | e-1$, thus $e \equiv 1 \pmod{\lambda(n)}$.

These remarks prove:

Proposition 5 *The RSA encryption functions E_e form a subgroup $H_n \leq \mathfrak{S}(M)$ that is isomorphic with $\mathbb{M}_{\lambda(n)}$ and has order $\varphi(\lambda(n))$ and exponent $\lambda(\lambda(n))$.*

Of course the order of a single encryption function E_e could be even much smaller: All we can say is that the cyclic subgroup $\langle e\rangle \leq \mathbb{M}_{\lambda(n)}$ has order $s := \operatorname{ord}(e) \mid \lambda(\lambda(n))$.

This observation raises two problems:

1. How large is $\lambda(\lambda(n))$?
2. Under what conditions is $\operatorname{ord}(e) = \lambda(\lambda(n))$? Or at least not significantly smaller?

Answer to 1 (without proof): “In general” $\lambda(\lambda(n)) \approx \frac{n}{8}$.

If we want to be sure about this we should choose p, q as special primes $p = 2p' + 1$, $q = 2q' + 1$ with different primes $p', q' \geq 3$. Then for $n = pq$ we have

$$\lambda(n) = \mathrm{kgV}(2p', 2q') = 2p'q' = \frac{(p-1)(q-1)}{2} \approx \frac{n}{2}.$$

If moreover p and q are superspecial primes, that is, $p' = 2p'' + 1$ and $q' = 2q'' + 1$ are special primes too, then

$$\lambda(\lambda(n)) = 2p''q'' = \frac{(p-3)(q-3)}{8} \approx \frac{n}{8}.$$

By the prime number theorem, see Section 2.1, we may expect that superspecial primes exist in astronomic quantities.

Answer to 2: in most cases (also without general proof).

Again, if we want to be sure, we should confine our choices to special or even superspecial primes. We use some elementary results on finite groups, see Lemmas 21, 22, and 23 of Appendix A.10.

Let p be an odd prime number. In the additive cyclic group $\mathbb{Z}/2p\mathbb{Z}$ we consider the subsets:

$$\begin{aligned} E_p &= \{a \bmod 2p \mid 0 \leq a < p,\ a \text{ even}\} - \{0\}, \\ O_p &= \{a \bmod 2p \mid 0 \leq a < p,\ a \text{ odd}\} - \{p\}. \end{aligned}$$

Clearly, $\mathbb{Z}/2p\mathbb{Z} = \{0, p\} \cup E_p \cup O_p$, and

$$\#E_p = \#O_p = p - 1.$$

The order of an element $x \in \mathbb{Z}/2p\mathbb{Z}$ is

$$\operatorname{ord} x = \begin{cases} 1 & \Longleftrightarrow x = 0, \\ 2 & \Longleftrightarrow x = p, \\ p & \Longleftrightarrow x \in E_p, \\ 2p & \Longleftrightarrow x \in O_p. \end{cases}$$

We transfer this result to an abstract cyclic group $\mathcal{Z}_{2p}$ with generating element g via the isomorphism

$$\tau : \mathbb{Z}/2p\mathbb{Z} \longrightarrow \mathcal{Z}_{2p}, \quad x \mapsto g^x.$$

Let $\mathcal{E}_p = \tau E_P$ and $\mathcal{O}_p = \tau O_P$. Then the result is:

Lemma 2 *The order of an element $h \in \mathcal{Z}_{2p}$ is*

$$\operatorname{ord} h = \begin{cases} 1 & \Longleftrightarrow h = \mathbf{1}, \\ 2 & \Longleftrightarrow h = g^p, \\ p & \Longleftrightarrow h \in \mathcal{E}_p, \\ 2p & \Longleftrightarrow h \in \mathcal{O}_p. \end{cases}$$

Next we study the orders of the elements of the direct product $\mathcal{Z}_{2p} \times \mathcal{Z}_{2q}$ for two different odd primes p and q. Applying Lemma 21 we see that the order of a pair (g, h) for $g \in \mathcal{Z}_{2p}$ and $h \in \mathcal{Z}_{2q}$ is given by the following table:

		$\operatorname{ord} g =$			
		1	2	p	$2p$
$\operatorname{ord} h =$	1	1	2	p	$2p$
	2	2	2	$2p$	$2p$
	q	q	$2q$	pq	$2pq$
	$2q$	$2q$	$2q$	$2pq$	$2pq$

An obvious count yields:

Proposition 6 *Let p and q be two different odd primes. Then the direct product group $\mathcal{Z}_{2p} \times \mathcal{Z}_{2q}$ has*

(i) 1 *element of order* 1,

(ii) 3 *elements of order* 2,

(iii) $p - 1$ *elements of order* p,

(iv) $3 \cdot (p - 1)$ *elements of order* $2p$,

(v) $q - 1$ *elements of order* q,

(vi) $3 \cdot (q - 1)$ *elements of order* $2q$,

(vii) $(p - 1) \cdot (q - 1)$ *elements of order* pq,

(viii) $3 \cdot (p - 1) \cdot (q - 1)$ *elements of order* $2pq$.

Again let p be a prime number. Then the multiplicative group $\mathbb{M}_p = (\mathbb{Z}/p\mathbb{Z})^\times$ of the finite field $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$. Let q be a prime different from p and let $n = p \cdot q$. Then by the Chinese Remainder Theorem $\mathbb{M}_n \cong \mathbb{M}_p \times \mathbb{M}_q$ is (up to isomorphy) the direct product of two cyclic groups of orders $p-1$ and $q-1$. Hence:

Lemma 3 *Let $n = pq$ be the product of two different odd primes p and q. Then the multiplicative group $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ of the quotient ring $\mathbb{Z}/n\mathbb{Z}$ has order $\varphi(n) = (p-1)(q-1)$ and exponent $\lambda(n) = \operatorname{lcm}(p-1, q-1)$. In particular $\mathbb{M}_n$ is not cyclic.*

The latter statement is due to the common divisor 2 of $p-1$ and $q-1$.

We now consider the case where $p = 2p' + 1$ and $q = 2q' + 1$ are special primes. Then

$$\varphi(n) = 4p'q' \quad \text{and} \quad \lambda(n) = 2p'q'.$$

By Proposition 5 the RSA encryption functions for the module $n = pq$ make up a group H_n isomorphic with $\mathbb{M}_{\lambda(n)}$. For special primes we therefore have by Theorem 2 in Appendix A.4:

Proposition 7 *Let $n = pq$ be the product of two different special primes $p = 2p' + 1$ and $q = 2q' + 1$. Then the RSA group*

$$H_n \cong \mathbb{M}_{\lambda(n)} \cong \mathcal{Z}_{p'-1} \times \mathcal{Z}_{q'-1}$$

is the product of two cyclic groups of orders $p' - 1$ and $q' - 1$.

In order to derive some more easy results we assume that p and q are superspecial primes, with $p' = 2p'' + 1$ and $q' = 2q'' + 1$. Then

$$H_n \cong \mathbb{M}_{\lambda(n)} \cong \mathcal{Z}_{2p''} \times \mathcal{Z}_{2q''},$$

and Proposition 6 applies for the primes p'' and q'':

Proposition 8 *Let $n = pq$ be the product of two different superspecial primes $p = 2p' + 1$ and $q = 2q' + 1$ with $p' = 2p'' + 1$ and $q' = 2q'' + 1$. Then the RSA group H_n consists of*

(i) 1 *element of order* 1,

(ii) 3 *elements of order* 2,

(iii) $p'' - 1$ *elements of order* p'',

(iv) $3 \cdot (p'' - 1)$ *elements of order* $2p''$,

(v) $q'' - 1$ *elements of order* q'',

(vi) $3 \cdot (q'' - 1)$ *elements of order* $2q''$,

(vii) $(p'' - 1) \cdot (q'' - 1)$ *elements of order* $p''q''$,

(viii) $3 \cdot (p'' - 1) \cdot (q'' - 1)$ *elements of order* $2p''q''$.

Since $2p''q'' = \lambda(\lambda(n))$ is the exponent of H_n we see that almost all of its elements have their orders near the maximum. More precisely the number of elements of order $< \frac{1}{2}\,\lambda(\lambda(n)) = p''q''$ is

$$1 + 3 + 4 \cdot (p'' - 1) + 4 \cdot (q'' - 1) = 4 \cdot (p'' + q'' - 1).$$

Corollary 1 *The number of elements of* H_n *with order* $< \frac{1}{2}\,\lambda(\lambda(n))$ *is* $p + q - 7$.

Proof. Note that $p'' = (p - 3)/4$. ◇

Thus this number is $\approx 2 \cdot \sqrt{n}$ if p and q—as recommended in Section 2.4—are chosen near $\sqrt{n}$. Then the proportion of elements of "small" orders is $\approx 2/\sqrt{n}$, and this proportion asymptotically tends to 0 with growing values of n.

As a consequence we resume: *With negligeable exceptions s has the order of magnitude of $n/8$.* The best known general results are in Chapter 23 of Shparlinski's book, see the references for these lecture notes.

In addition to Section 2.2 we formulate the task

(F) Finding the order s of the encryption function.

In the sense of complexity theory we have the implication

$$(\mathrm{F}) \longrightarrow (\mathrm{A})$$

but maybe not the reverse implication. If the order s is known, then $D = E^{s-1}$ and thus $d = e^{s-1}$ are efficiently computable. *Finding the order of the encryption function is at least as difficult as factoring the module.*