4'th turorial: Attacks on the RSA-protocol

Ex: Bob's public key is $(n, e_B) = (91, 11)$, Cecilia's public key is $(n, e_c) = (91, 5)$. Alice has send a message $b = 31$ to Bob. Cecilia knows her private key $(n, d_c) = (91, 29)$, she does an insider attack and factorizes n. Finally she decrypts the message.

$e_c d_c - 1 = 5 \cdot 29 - 1 = 144 = 2^4 \cdot 9$

For $\underline{a}$ relatively prime to $\underline{n} = 91$ is $a^{ed-1} = a^{144} = 1$ in $\mathbb{Z}_{91}$

We choose $a = 2$: $2 \xrightarrow{(\ )^9} 512 = 57 \xrightarrow{s} 3249 = 64 \xrightarrow{s} 4096 = 1$

OK, we found non-triv. $\sqrt{1}$: $b = 64$

we count $\gcd(b-1, n) = \gcd(63, 91) = 7$

Eukleid: $91 = 63 + 28$
$63 = 2 \cdot 28 + 7$
$28 = 4 \cdot 7 + 0$

Factorization $n = 91 = 7 \cdot 13$.

Bob's private key : $\varphi(n) = 6 \cdot 12 = 72$

$d_B = 11^{-1}$ in $\mathbb{Z}_{72}$

$11 d_B + 72 k = 1$ in $\mathbb{Z}$

$$\left(\begin{array}{cc|c} 1 & 0 & 11 \\ 0 & 1 & 72 \end{array}\right) \sim \left(\begin{array}{cc|c} -13 & 2 & 1 \\ -7 & 1 & -5 \end{array}\right) \begin{array}{l} R_1 + 2\check{R}_2 \\ R_2 - 7R_1 = \check{R}_2 \end{array}$$

$-13 \cdot 11 + 2 \cdot 72 = 1$

$d_B = -13 = 59$ in $\mathbb{Z}_{72}$

Decryption of $b = 31$

- we count residually $\mathbb{Z}_{91} \cong \mathbb{Z}_7 \times \mathbb{Z}_{13}$

in $\mathbb{Z}_7$: $a = b^{d_B} = 31^{59} = 3^{59} = 3^5 = 9^2 \cdot 3 = 4 \cdot 3 = 5$

E.-F.: we count mod $\varphi(7) = 6$ in the exponent

in $\mathbb{Z}_{13}$: $a = b^{d_B} = 31^{59} = 5^{-1} = -5 = 8$, since $5 \cdot (-5) = -25 = 1$ in $\mathbb{Z}_{13}$

E.-F.: we count mod $\varphi(13) = 12$ in the exponent

↳ Chinese remainder th.

in $\mathbb{Z}_{91}$ $a = 5 \cdot q_7 + 8 q_{13} = 5 \cdot (-13) + 8 \cdot 14 = 47$

where $\underbrace{13 \cdot t}_{q_7 = -13} + \underbrace{7 r}_{q_{13} = 14} = 1$ (we guess)

Open message: $\underline{a = 47}$.

Ex: Bob's public key is $(n, e_B) = (91, 11)$ again and Cecilia's public key $(n, e_C) = (91, 5)$. They both received the same message $\underline{a}$ from their boss. Eva eavesdropped the encrypted message for Bob $b_B = 46$ and for Cecilia $b_C = 32$. Eva counted the open message $\underline{a}$ by an outsider attack.

Bezout's th.: $\gcd(e_B, e_C) = \gcd(11, 5) = 1 = t \cdot 11 + s \cdot 5$ for $t, s \in \mathbb{Z}$.

we guess $t = 1,\ s = -2$

in $\mathbb{Z}_n = \mathbb{Z}_{91}$: $a = a^1 = a^{1\cdot 11 - 2\cdot 5} = a^{11} \cdot (a^5)^{-2} = b_B \cdot b_C^{-2} = 46 \cdot (32^{-1})^2 = \dots$ ⊛

we count $32^{-1} = x$ in $\mathbb{Z}_{91}$

$32x + 91y = 1$

$$\left(\begin{array}{cc|c} 1 & 0 & 32 \\ 0 & 1 & 91 \end{array}\right) \sim \left(\begin{array}{cc|c} -17 & 6 & 2 \\ -3 & 1 & -5 \end{array}\right) \begin{array}{l} R_1 + 6\check{R}_2 \\ R_2 - 3R_1 = \check{R}_2 \end{array} \sim \left(\begin{array}{cc|c} \cdot & \cdot & \cdot \\ -54 & 19 & 1 \end{array}\right) \begin{array}{l} \\ R_2 + 3R_1 \end{array}$$

$x = 32^{-1} = -54 = 37$ in $\mathbb{Z}_{91}$ $\qquad \underbrace{-54}_{x} \cdot 32 + 19 \cdot 91 = 1$

⊛ $a = 46 \cdot 37^2 = 46 \cdot 4 = 184 = 2$ the open message

Ex: The same situation as above only a different message: $b_B = 65$, $b_C = 65$.

in $\mathbb{Z}_{91}$: $a = b_B \cdot b_C^{-2} = 65 \cdot (65^{-1})^2 = 65^{-1}$

we count $65^{-1} = x$ in $\mathbb{Z}_{91}$

$$\left(\begin{array}{cc|c} 1 & 0 & 65 \\ 0 & 1 & 91 \end{array}\right) \sim \left(\begin{array}{cc|c} 3 & -2 & 13 \\ -1 & 1 & 26 \end{array}\right) \begin{array}{l} R_1 - 2\check{R}_2 \\ R_2 - R_1 = \check{R}_2 \end{array} \sim \left(\begin{array}{cc|c} 3 & -2 & 13 \\ -7 & 5 & 0 \end{array}\right) R_2 - 2 \ldots$$

$3 \cdot 65 - 2 \cdot 91 = 13$

We found that 65^{-1} does not exist in $\mathbb{Z}_{91}$, but we found factorization $n = 91 = 13 \cdot 7$. $\qquad \gcd(65, 91) = 13$

So Eve can count the private key of Bob and decrypt residually (as in the previous exercise). The result is $\underline{a = 39}$.

Ex: Three partitipants of an RSA-protocol have got the same modulus n,

$(n, e_1) = (247, 35)$, $(n, e_2) = (247, 55)$, $(n, e_3) = (247, 77)$.

The same message was sent to each of them and Eva heart these encrypted messages: $b_1 = 227$, $b_2 = 132$, $b_3 = 189$.

Eva did an outsider attack and decrypted the message.

$\gcd(35, 55) = 5$, $\gcd(55, 77) = 11$, $\gcd(35, 77) = 7$

only $\gcd(35, 55, 77) = 1$

Bezout's th.: $1 = t \cdot 35 + r \cdot 55 + s \cdot 77$ for $t, r, s \in \mathbb{Z}$.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 35 \\ 0 & 1 & 0 & 55 \\ 0 & 0 & 1 & 77 \end{array}\right) \sim \left(\begin{array}{ccc|c} \cdot & \cdot & \cdot & \cdot \\ 16 & 1 & -8 & -1 \\ -2 & 0 & 1 & 7 \end{array}\right) \begin{array}{l} R_2 - 8\check{R}_3 \\ R_3 - 2R_1 = \check{R}_3 \end{array}$$

$$-16 \cdot 35 - 1 \cdot 55 + 8 \cdot 77 = 1$$

in $\mathbb{Z}_n = \mathbb{Z}_{247}$ $\quad a = a^1 = b_1^{-16} \cdot b_2^{-1} \cdot b_3^{8} = (227^{-1})^{16} \cdot (132^{-1}) \cdot 189^{8} =$

$$= \ldots = 37^{16} \cdot 189 \cdot 189^{8} = \ldots = 37$$

Open message: $a = 37$.

Ex: Find a continued fraction for $\frac{a}{b} = \frac{73}{15}$ and evaluate its convergents.

Eukleid:

$73 = 4 \cdot 15 + 13$

$15 = 1 \cdot 13 + 2$

$13 = 6 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$$\frac{a}{b} = \frac{73}{15} = 4 + \frac{13}{15} = 4 + \frac{1}{\frac{15}{13}} = 4 + \frac{1}{1 + \frac{2}{13}} = \ldots$$

$$\ldots = 4 + \cfrac{1}{1 + \cfrac{1}{6 + \frac{1}{2}}}$$

We write shorter

$$\frac{73}{15} = (4; 1, 6, 2)$$

Convergents:

$(4) = 4$

$(4; 1) = 4 + \frac{1}{1} = 5$

$(4; 1, 6) = 4 + \cfrac{1}{1 + \frac{1}{6}} = 4 + \frac{6}{7} = \frac{34}{7}$

$(4; 1, 6, 2) = \ldots = \frac{73}{15}$

- convergents really convergate to $\frac{a}{b}$; longer convergent - better approximation

Ex: The public key of an RSA protocol is $(n, e) = (55\,751, 22109)$.
Use the Wiener's attack to count the private key.

The Wiener's attack works if primes are close and the private key is small.

If $q < p < 2q$, $d < \frac{1}{3}\sqrt[4]{n}$,

then from $ed = 1 + k\varphi(n)$

we have $\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{2d^2}$, $\gcd(k, d) = 1$,

which ensures that $\frac{k}{d}$ is a convergent of the continued fraction for $\frac{e}{n}$.

Continued fraction for $\frac{e}{n} = \frac{22\,109}{55\,751}$ is:

Euklid: $e = 0n + e$

$$55\,751 = 2 \cdot 22109 + 11\,533$$
$$22\,109 = 1 \cdot 11533 + 10\,576$$
$$11\,533 = 1 \cdot 10576 + 957$$
$$10\,576 = 11 \cdot 957 + 49$$
$$957 = 19 \cdot 49 + 26$$
$$49 = 1 \cdot 26 + 23$$
$$26 = 1 \cdot 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$$\frac{e}{n} = \frac{22\,109}{55\,751} = (0; 2, 1, 1, 11, 19, 1, 1, 7, 1, 2)$$

Convergents = suggestions for $\frac{k}{d}$, and for each we count $\varphi(n) = \frac{ed - 1}{k}$:

$(0) = 0$

$(0; 2) = \frac{1}{2}$ .... $\varphi(n) = \frac{e \cdot 2 - 1}{1} = 44\,217$ NO (since $\varphi(n)$ should be even)

$(0; 2, 1) = \frac{1}{2 + \frac{1}{1}} = \frac{1}{3}$ .... $\varphi(n) = \frac{e \cdot 3 - 1}{1} = 66\,326$ NO (since $\varphi(n) < n$)

$(0; 2, 1, 1) = \frac{1}{2 + \frac{1}{1 + \frac{1}{1}}} = \frac{2}{5}$ ... $\varphi(n) = \frac{e \cdot 5 - 1}{2} = 55\,272$ MAYBE YES

$(0; 2, 1, 1, 11) = \ldots = \frac{23}{58}$ ... $\varphi(n) = \frac{e \cdot 58 - 1}{23} = \frac{1282321}{23}$ NO (since $\varphi(n) \notin \mathbb{N}$)

$(0; 2, 1, 1, 11, 19) = \frac{439}{1107}$ ... $\varphi(n) = \frac{2447462}{901}$ NO (here $\varphi(n) \notin \mathbb{N}$)

Note: $\sqrt[4]{n} \doteq \cancel{15}$, Wiener's attack could work for $d < \sqrt[2]{n} \doteq 236$

Denominator of convergents increases, we have $d = 1107$ already, so we stop our looking for good possibilities.

Possibility $\frac{k}{d} = \frac{2}{5}$ gives $\varphi(n) = 55272$ for $n = 55751$.

We try to factorize $n = pq$ using $\varphi(n) = pq - (p+q) + 1$.

$p + q = n - \varphi(n) + 1 = 480$

p, q solve the equation $x^2 - 480x + 55751 = 0$

$D = 7396$, $\sqrt{D} = 86$

$p, q = \frac{480 \pm 86}{2} = \begin{cases} 197 \\ 283 \end{cases}$ both are primes

Thus $n = 197 \cdot 283$

$\varphi(n) = 55272$

and the private key $\underline{d = 5}$.

Homework:

1) (Insider attack) Three partitipants of an RSA protocol have got public keys with the same modulus: $(n, e_1) = (4369, 17)$, $(n, e_2) = (4369, 5)$, $(n, e_3) = (4369, 75)$. As the first one you know your private key $(n, d_1) = (4369, 241)$. Factorize the modulus n and count private keys of the others.
[$n = 17 \cdot 257$, $d_2 = 3277$, $d_3 = 2403$]

2) (Outsider attack) Two partitipants of an RSA protocol have got public keys with the same modulus: $(n, e_1) = (1037, 23)$, $(n, e_2) = (1037, 7)$. The same message $\underline{a}$ was sent to both of them, the first one has received the encrypted message $b_1 = 21$, the second one $b_2 = 395$. Use outsider attack to count the open message $\underline{a}$.
Do it once again for $\bar{b}_1 = 935$, $\bar{b}_2 = 119$. [$a = 642$, $\bar{a} = 34$]

3) (Hastad's attack) The same open message $\underline{a}$ was sent to three partitipants with public keys: $(n_1, e) = (205, 3)$, $(n_2, e) = (319, 3)$, $(n_3, e) = (391, 3)$. The first one has received the encrypted message $b_1 = 82$, the second one $b_2 = 140$ and the third one $b_3 = 98$. Use the Hastad's attack to count the message $\underline{a}$.

[$a = 123$]