Problems with Schoolbook RSA II

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Related messages and small exponent

Given two ciphertexts c_1, c_2 encrypted to $(n, 3)$.
If $m_2 = am_1 + b$ for known a, b and unknown m_1 we can recover m_1 from the ciphertexts:

Related messages and small exponent

Given two ciphertexts c_1, c_2 encrypted to $(n, 3)$.
If $m_2 = am_1 + b$ for known a, b and unknown m_1 we can recover m_1 from the ciphertexts:

Note that $c_2 = (am_1 + b)^3 = a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3$.

Put

$$A = b(c_2 + 2a^3 c_1 - b^3)$$

Related messages and small exponent

Given two ciphertexts c_1, c_2 encrypted to $(n, 3)$.
If $m_2 = am_1 + b$ for known a, b and unknown m_1 we can recover m_1 from the ciphertexts:

Note that $c_2 = (am_1 + b)^3 = a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3$.

Put

$$\begin{aligned} A &= b(c_2 + 2a^3 c_1 - b^3) \\ &= b(a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3 + 2a^3 m_1^3 - b^3) \\ &= 3abm_1(a^2 m_1^2 + am_1 b + b^2) \end{aligned}$$

and

$$B = a(c_2 - a^3 c_1 + 2b^3)$$

Related messages and small exponent

Given two ciphertexts c_1, c_2 encrypted to $(n, 3)$.
If $m_2 = am_1 + b$ for known a, b and unknown m_1 we can recover m_1 from the ciphertexts:

Note that $c_2 = (am_1 + b)^3 = a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3$.

Put

$$\begin{aligned} A &= b(c_2 + 2a^3 c_1 - b^3) \\ &= b(a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3 + 2a^3 m_1^3 - b^3) \\ &= 3abm_1(a^2 m_1^2 + am_1 b + b^2) \end{aligned}$$

and

$$B = a(c_2 - a^3 c_1 + 2b^3) = 3ab(a^2 m_1^2 + am_1 b + b^2).$$

Related messages and small exponent

Given two ciphertexts c_1, c_2 encrypted to $(n, 3)$.
If $m_2 = am_1 + b$ for known a, b and unknown m_1 we can recover m_1 from the ciphertexts:

Note that $c_2 = (am_1 + b)^3 = a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3$.

Put

$$\begin{aligned} A &= b(c_2 + 2a^3 c_1 - b^3) \\ &= b(a^3 m_1^3 + 3a^2 m_1^2 b + 3am_1 b^2 + b^3 + 2a^3 m_1^3 - b^3) \\ &= 3abm_1(a^2 m_1^2 + am_1 b + b^2) \end{aligned}$$

and

$$B = a(c_2 - a^3 c_1 + 2b^3) = 3ab(a^2 m_1^2 + am_1 b + b^2).$$

Thus $A/B = m$.
(Note: all computations are done modulo n).

Generalizations

This gets more messy for larger e – but that won't stop an attacker.

Generalizations

This gets more messy for larger e – but that won't stop an attacker.

Let c_1 and c_2 be encryptions related to m.

Let $f(x, c_1, c_2)$ and $g(x, c_1, c_2)$ be such that

$$f(m, c_1, c_2) = g(m, c_1, c_2) = 0.$$

Generalizations

This gets more messy for larger e – but that won't stop an attacker.

Let c_1 and c_2 be encryptions related to m.

Let $f(x, c_1, c_2)$ and $g(x, c_1, c_2)$ be such that

$$f(m, c_1, c_2) = g(m, c_1, c_2) = 0.$$

Then most likely $\gcd(f(x, c_1, c_2), g(x, c_1, c_2)) = x - m$ (up to scaling.

Finding f and g depends on relation.

Generalizations

This gets more messy for larger e – but that won't stop an attacker.

Let c_1 and c_2 be encryptions related to m.

Let $f(x, c_1, c_2)$ and $g(x, c_1, c_2)$ be such that

$$f(m, c_1, c_2) = g(m, c_1, c_2) = 0.$$

Then most likely $\gcd(f(x, c_1, c_2), g(x, c_1, c_2)) = x - m$ (up to scaling.

Finding f and g depends on relation.

Easier with more messages (see exercise 6 on sheet 5).