Problems with Schoolbook RSA I

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Small exponent RSA

Often e is chosen so that computing $m^e \bmod n$ is fast.
This means e is small and has a low Hamming weight
(Hamming weight = number of 1s in the binary representation).

Typical choices: $e \in \{3, 17, 65537\}$.

Small exponent RSA

Often e is chosen so that computing $m^e \bmod n$ is fast.
This means e is small and has a low Hamming weight
(Hamming weight = number of 1s in the binary representation).

Typical choices: $e \in \{3, 17, 65537\}$.
$65537 = 2^{16} + 1$.

Obvious problem:
If e and m are small then $c = m^e$ (no reduction modulo n),
and integer e-th powers are easy to spot and to undo.

E.g. $c = 4096$ for $(n, e) = (663847, 3)$.

Small exponent RSA

Often e is chosen so that computing $m^e \bmod n$ is fast.
This means e is small and has a low Hamming weight
(Hamming weight = number of 1s in the binary representation).

Typical choices: $e \in \{3, 17, 65537\}$.
$65537 = 2^{16} + 1$.

Obvious problem:
If e and m are small then $c = m^e$ (no reduction modulo n),
and integer e-th powers are easy to spot and to undo.

E.g. $c = 4096$ for $(n, e) = (663847, 3)$.
We know $4096 = 2^{12} = 2^{3 \cdot 4} = 16^3$, thus $m = 16$.

Small exponent RSA

Often e is chosen so that computing $m^e \bmod n$ is fast.
This means e is small and has a low Hamming weight
(Hamming weight = number of 1s in the binary representation).

Typical choices: $e \in \{3, 17, 65537\}$.
$65537 = 2^{16} + 1$.

Obvious problem:
If e and m are small then $c = m^e$ (no reduction modulo n),
and integer e-th powers are easy to spot and to undo.

E.g. $c = 4096$ for $(n, e) = (663847, 3)$.
We know $4096 = 2^{12} = 2^{3 \cdot 4} = 16^3$, thus $m = 16$.

This problem can be fixed by padding so that encoded messages are large enough.

CRT attack on low-exponent Schoolbook RSA encryption

Patty is organizing a party and is inviting friends Alice, Bob, and Charlie. She uses Schoolbook RSA encryption to send them the date of the party. Their keys are (n_A, e), $(n_B, 3)$, and $(n_C, 3)$.

Eve is not invited but has the ciphertexts

$$\begin{aligned} c_A &\equiv m^3 \bmod n_A \\ c_B &\equiv m^3 \bmod n_B \\ c_C &\equiv m^3 \bmod n_C \end{aligned}$$

CRT attack on low-exponent Schoolbook RSA encryption

Patty is organizing a party and is inviting friends Alice, Bob, and Charlie. She uses Schoolbook RSA encryption to send them the date of the party. Their keys are (n_A, e), $(n_B, 3)$, and $(n_C, 3)$.

Eve is not invited but has the ciphertexts

$$\begin{aligned} c_A &\equiv m^3 \bmod n_A \\ c_B &\equiv m^3 \bmod n_B \\ c_C &\equiv m^3 \bmod n_C \end{aligned}$$

Using the Chinese Remainder Theorem, she can compute

$$m^3 \bmod n_A n_B n_C.$$

CRT attack on low-exponent Schoolbook RSA encryption

Patty is organizing a party and is inviting friends Alice, Bob, and Charlie. She uses Schoolbook RSA encryption to send them the date of the party. Their keys are (n_A, e), $(n_B, 3)$, and $(n_C, 3)$.

Eve is not invited but has the ciphertexts

$$\begin{aligned} c_A &\equiv m^3 \bmod n_A \\ c_B &\equiv m^3 \bmod n_B \\ c_C &\equiv m^3 \bmod n_C \end{aligned}$$

Using the Chinese Remainder Theorem, she can compute

$$m^3 \bmod n_A n_B n_C.$$

She notes that m is smaller than each of the n, so $m^3 < n_A n_B n_C$.

CRT attack on low-exponent Schoolbook RSA encryption

Patty is organizing a party and is inviting friends Alice, Bob, and Charlie. She uses Schoolbook RSA encryption to send them the date of the party. Their keys are (n_A, e), $(n_B, 3)$, and $(n_C, 3)$.

Eve is not invited but has the ciphertexts

$$\begin{aligned} c_A &\equiv m^3 \bmod n_A \\ c_B &\equiv m^3 \bmod n_B \\ c_C &\equiv m^3 \bmod n_C \end{aligned}$$

Using the Chinese Remainder Theorem, she can compute

$$m^3 \bmod n_A n_B n_C.$$

She notes that m is smaller than each of the n, so $m^3 < n_A n_B n_C$. Which means that she has an *integer cube* without reduction.

Example

The keys are $(n_A, e) = (663847, 3)$, $(n_B, 3) = (622411, 3)$, and $(n_C, 3) = (499153, 3)$.

The ciphertexts are: $c_A = 94601, c_B = 380254, c_C = 451506$.
CRT computation gives

$$m^3 \equiv 19951021419848000 \bmod n_A n_B n_C$$

and thus $m = 271220$.

Example

The keys are $(n_A, e) = (663847, 3)$, $(n_B, 3) = (622411, 3)$, and $(n_C, 3) = (499153, 3)$.

The ciphertexts are: $c_A = 94601, c_B = 380254, c_C = 451506$.
CRT computation gives

$$m^3 \equiv 19951021419848000 \bmod n_A n_B n_C$$

and thus $m = 271220$.

The same works for exponent e if Eve gets e ciphertexts of the same message, all using e.

Example

The keys are $(n_A, e) = (663847, 3)$, $(n_B, 3) = (622411, 3)$, and $(n_C, 3) = (499153, 3)$.

The ciphertexts are: $c_A = 94601, c_B = 380254, c_C = 451506$.
CRT computation gives

$$m^3 \equiv 19951021419848000 \bmod n_A n_B n_C$$

and thus $m = 271220$.

The same works for exponent e if Eve gets e ciphertexts of the same message, all using e.

Solution: randomized padding.