RSA. RSA Cryptosystem


(RSA.1) Let \( p, q \) be two distinct primes and \( n = pq \). Let \( e > 0 \) be an integer so that
\[
(e, \phi(n)) = (e, (p - 1)(q - 1)) = 1,
\]
and \( d \) be an integer such that \( de \equiv 1 \pmod{\phi(n)} \). For an integer \( m \) with \( \gcd(m, n) = 1 \), if \( c \equiv m^e \pmod{n} \), then \( m \equiv c^d \pmod{n} \).

**Proof:** As \( de \equiv 1 \pmod{\phi(n)} \), for some integer \( k \), we can write \( de = 1 + k\phi(n) \). Thus
\[
c^d \equiv (m^e)^d \equiv m^{de} \equiv m^{1+k\phi(n)} \equiv m \cdot (m^{\phi(n)})^k \pmod{n}.
\]
By \( \gcd(m, n) = 1 \) and by Euler’s theorem, \( m^{\phi(n)} \equiv 1 \pmod{n} \), and so
\[
c^d \equiv m \pmod{n}.
\]

(RSA.2) Assume that \( p, q, n, e, d \) are the same as in (RSA.1). Let \( m \) and \( s \) be integers, and suppose that \( s \equiv 0 \pmod{\phi(n)} \).

(i) If \( \gcd(m, n) = 1 \), then both \( m^s \equiv 1 \pmod{p} \) and \( m^s \equiv 1 \pmod{q} \).

(ii) Even \( \gcd(m, n) \neq 1 \), we still have both \( m^{s+1} \equiv m \pmod{p} \) and \( m^{s+1} \equiv m \pmod{q} \).

(iii) In any case, \( m^{ed} \equiv m \pmod{n} \).

**Proof:** (i) Note that \( n = pq \) and so \( \phi(n) = (p - 1)(q - 1) \). Thus from \( s \equiv 0 \pmod{\phi(n)} \), we can write \( s = t(p - 1)(q - 1) \) for some integer \( t \). It follows by Fermat that
\[
m^s \equiv m^{t(p-1)(q-1)} = (m^{p-1})^{t(q-1)} \equiv 1^{t(q-1)} \equiv 1 \pmod{p}.
\]
Similarly, \( m^s \equiv 1 \pmod{q} \).

(ii) We may assume that \( \gcd(m, n) \neq 1 \), otherwise (ii) follows from (i) by multiplying both sides of \( m^s \equiv 1 \pmod{p} \) and both sides of \( m^s \equiv 1 \pmod{q} \) by \( a \), respectively.

Since \( n = pq \), \( \gcd(m, n) \) must be either \( p \), or \( q \), or \( n \). Therefore, we can write \( m = tp \) for some integer \( t \) (or \( m = tq \) for some integer \( t \), respectively). It follows that \( m^{s+1} \equiv 0 \equiv m \pmod{p} \) (or \( m^{s+1} \equiv 0 \equiv m \pmod{q} \), respectively).

(iii) Note that \( ed \equiv 1 \pmod{\phi(n)} \). Let \( s = ed - 1 \). Then \( s \equiv 0 \pmod{\phi(n)} \), and so by (ii), both \( m^{s+1} \equiv m \pmod{p} \) and \( m^{s+1} \equiv m \pmod{q} \) hold. It follows by \( \gcd(p, q) = 1 \) that
\[
m^{ed} \equiv m^{s+1} \equiv m \pmod{n}.
\]
(RSA.3) The RSA Algorithm

**Choose System Parameters**  Choose two primes $p$ and $q$, and let $n = pq$. Pick an integer $e$ between 1 and $\phi(n)$ so that
\[(e, \phi(n)) = (e, (p - 1)(q - 1)) = 1.\]

**Make Encryption and Decryption Keys**  Compute $d \equiv e^{-1} \pmod{\phi(n)}$. Then
\[K_E = (n, e), \text{ and } K_D = (n, d).\]

**The Encoding and Decoding Process**  Let Alice and Bob be the two players in the system: the message sender (Alice) and the recipient (Bob).

1. Bob produces the encryption and decryption keys $K_E$ and $K_D$, and he let Alice know $K_E$. (He might let all potential message senders know $K_E$ and so he publicizes $K_E$ in this sense). But Bob keeps $K_D$ as a secret.
2. When Alice wants to send Bob a message $P$, Alice would first compute
\[C \equiv P^e \pmod{n},\]
and then send $C$ to Bob.
3. Receiving a coded message $c$ from $A$, $B$ can recover the original message $m \equiv c^d \pmod{n}$, by (RSA.2).

(RSA.4) **Example:** (encryption of a single number) Let $p = 167$, $q = 547$, $n = 91349$, $e = 5$ and cipher text $c \equiv 88291 \pmod{n}$. To find plain text $m$, we first find $\phi(n) = 90636$, and compute (using Euclidean Algorithm)
\[1 = \gcd(5, 90636) = 5(72509) + (-4)(90636),\]
and so $d = 72509$. Then
\[m = c^d \equiv 88291^{72509} \equiv 12345 \pmod{n}.\]

(RSA.5) **Example:** (encryption using blocks of size 3, or trigraphs) Let $p = 281$, $q = 167$. Then $n = 46927$. Pick $e = 39423$. Thus the enciphering key is (46927, 39423) and the deciphering key is (46927, 26767). In order to use the English Alphabet in the messages, Bob also tells Alice to use base-$N$ representation of the numerics with $N = 26$. 

2
To send a message YES to Bob, Alice first finds the numerical equivalent of \( \text{YES} = (24)(4)(18) \mapsto P = 24(26)^2 + 4(26) + 18 = 16346 \) (in base-10). Next, Alice computes 
\[ C = P^m = 16346^{39423} \equiv 21166 \pmod{46927} \]
and then converts \( C \) to Base-26 numbers and their letter equivalents: 
\[ C = 1(26)^3 + 5(26)^2 + 8(26) + 2 \mapsto (1)(5)(8)(2) = \text{BFIC}. \]
And she transmits \( \text{BFIC} \) to Bob.

Receiving the message \( \text{BFIC} \) from Alice, Bob converts it back to base-10 numbers 
\[ \text{BFIC} = 21166, \]
then applies the deciphering key to compute 
\[ 21166^{26767} \equiv 16346 \pmod{46927}. \]
After he converts it to base-26 numbers, he recognizes that the message is \( \text{YES} \). (Who knows what he was asking Alice?)

(RSA.6) Consideration in choosing parameters

Let \( n = pq \), where \( p \) and \( q \) are primes with \( q < p < 2q \). Suppose that \( d < \frac{5\sqrt{n}}{3} \). If an integer \( e \) is known and if \( de \equiv 1 \pmod{\phi(n)} \), then there is an effective algorithm to compute \( d \).

(RSA.7) Breaking the System Parameters: Knowing that both \( n = pq \) is a product of two distinct primes (assuming \( p > q \)) and \( \phi(n) \), it is possible to factor \( n \), as following:

(Step 1) Use the following identities to compute \( p + q \) and \( p - q \).
\[
\begin{align*}
p + q &= n - (p - 1)(q - 1) + 1 = n - \phi(n) + 1. \\
p - q &= \sqrt{(p + q)^2 - 4n}
\end{align*}
\]

(Step 2) Compute \( p \) and \( q \).
\[
p = \frac{(p + q) + (p - q)}{2}, \quad q = \frac{(p + q) - (p - q)}{2}.
\]

Example: Knowing that \( pq = 1009427 \) and \( \phi(pq) = 1007400 \). We then compute \( p + q = 2028 \) and \( p - q = 274 \). Thus \( p = 1151 \) and \( q = 877 \).

(RSA.8) Impersonation Attack: Suppose that \( A \) sent a cipher text \( c \) to \( B \) using an RSA with encryption key \( K_E = (n, e) \). This message was intercepted by \( C \). \( C \) wants to compute \( m \) knowing that \( c \equiv m^e \pmod{n} \). To do that, \( C \) randomly select an \( x \in \mathbb{Z}_n^* \) and compute \( \bar{c} \equiv cx^e \pmod{n} \). Then \( C \) pretends to be \( A \) and send \( \bar{c} \) to \( B \).

Not knowing this, \( B \) receives \( \bar{c} \). He then computes \( \overline{m} \equiv \bar{c}^d \pmod{n} \) and sends \( \overline{m} \) back to \( A \). Now \( C \) can intercept \( \overline{m} \) and compute
\[
\overline{m} \equiv \bar{c}^d \equiv c^d \cdot (x^e)^d \equiv mx \pmod{n},
\]
and so \( C \) can find out \( m \). This attack is also called a Chosen-Cipher Text Attack.
RSA Digital Signature

**System parameters:** Let $p, q$ be two distinct primes and let $n = pq$.

**Enciphering keys and redundancy function:** A picks a random number $e$ with $1 < e < \phi(n)$ such that $gcd(e, \phi(n)) = 1$. Then $A$ publicizes the encryption key $K_E(n, e)$. $A$ also picks a function $R : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ (called the redundancy function), which is also publicized.

**Decryption key:** $A$ computes $d = e^{-1} \pmod{\phi(n)}$.

**Signature of the message sender:** $A$ wants to send a message $m$ to $B$ with an electronic signature. $A$ first computes $R(m) = m'$ and then compute $s = (m')^d \pmod{n}$. Then $A$ sends the signed message $s$ to $B$.

**Verification of signature:** $B$ receives $s$ from $A$. Since $K_E(n, e)$ and $R$ are in the public domain, $A$ first computes $m' \equiv s^e \pmod{n}$. Then $B$ checks if $m'$ is in the range of $R$. If YES, the $B$ verifies $A$’s signature; if not $B$ consider this is not a message sent from $A$ and so rejects the message.

**Decoding:** Once the signature is verified, $m = R^{-1}(m')$ can be computed.

(RSA. 10) Example: Suppose that $n = 466727$ $\phi(n) = 465336$, $d = 296123$, $m = 10101$, and $c = 369510$. First compute $e \equiv d^{-1} \pmod{\phi(n)}$. For the given $m$ and $c$, define

$$
ver_k(m, c) = \begin{cases} 
1 & \text{if } m \equiv c^e \pmod{n} \\
0 & \text{if } m \not\equiv c^e \pmod{n} 
\end{cases}
$$

Verify the signature by either rejecting the message if $ver_k(m, c) = 0$ or accepting it if $ver_k(m, c) = 1$.

**Solution:** First compute (by Euclidean Algorithm)

$$
1 = gcd(296123, 465336) = (11)(296123) + (-7)(465336),
$$

and so $e = 11$. Then compute $c^{11} = 369510^{11} \equiv 369510 \pmod{n}$, and so we accept it.

(RSA. 11) Example: Suppose that $n = 1081357$ $\phi(n) = 1079260$, $d = 571313$, $m = 7381$, and $c = 725226$. Verify the signature.

**Solution:** First compute (by Euclidean Algorithm)

$$
1 = gcd(571313, 1079260) = (17)(571313) + (-9)(1079260),
$$

and so $e = 17$. Then compute $c^{17} = 725226^{17} \not\equiv 7381 \pmod{n}$, and so we reject it.

(RSA.12) ElGamal Public Key Cipher:

**Choosing System Parameters** A usually large prime $p$, a primitive root $a$ modulo $p$. 

4
**Making Enciphering and Deciphering Keys**  Pick an integer \( e \) with \( 1 < e < p - 1 \) and compute \( b \equiv a^e \pmod{p} \). The encryption key \( E_K = (p, a, b) \). The number \( e \) is the secret decryption key.

Bob makes all the above and he keeps \( e \) a secret. After he has done it, he publicizes the encryption key \( K_E \).

**Encoding Process**  When Alice wants to send Bob a message \( m \in \mathbb{Z}_p \) (we can view that \( m \in \mathbb{Z} \) with \( 0 \leq m < p \)), she does the following

(i) Download \( (p, a, b) \).
(ii) Pick a random (secret) number \( k \), and computes \( r \equiv a^k \pmod{p} \).
(iii) Compute \( t \equiv b^k m \pmod{p} \).
(iv) Send the ordered pair \( c = (r, t) \) to Bob.

**Decoding Process**  After receiving \( c = (r, t) \), Bob computes

\[
tr^{-e} \equiv b^k \cdot m \cdot a^{k(-e)} \equiv a^{ke} \cdot m \cdot a^{-ke} \equiv m \pmod{p}.
\]

**Remark:**  The assumption of this cryptosystem is that the discrete log problem is difficult, and so finding \( e = L_a(b) \), or finding \( k = L_b(r) \) are generally not easy.

(RSA. 13) **Example:**

**Choosing System Parameters**  Suppose that \( B \) chooses \( p = 3359, a = 11 \) and \( e = 5 \). He computes \( b = a^e = 11^5 \equiv 3187 \pmod{p} \), and publicists \( K_E = (p, a, b) = (3359, 11, 3178) \).

**Encoding Process**  \( A \) wants to send a message \( m = 2132 \) to \( B \). \( A \) downloads \( K_E = (3359, 11, 3178) \), and picks a random number \( k = 69 \), and computes

\[
r \equiv a^k = 11^{69} \equiv 193, \quad t \equiv b^k m \equiv 3178^{69} \cdot 2132 \equiv 2719 \pmod{p}.
\]

Then \( A \) sends \( c = (r, t) = (193, 2719) \) to \( B \).

**Decoding Process**  \( B \), after receiving \( c = (r, t) = (193, 2719) \), computes

\[
m \equiv tr^{-e} \equiv 2719 \cdot 193^{-5} \equiv 2132 \pmod{p}.
\]

(RSA. 14) **Example:**  Suppose \( A \) and \( B \) are using the ElGamal public-key cipher to communicate with \( p = 1213 \) and \( e = 15 \). Suppose \( A \) sends a cipher tex \( c = (661, 193) \) to \( B \). Find the plain text \( m \).

**Solution:**  Here \( t = 193 \) and \( r = 661 \). Compute

\[
r^{-e} \equiv 661^{-15} \equiv 924 \pmod{1213},
\]
and so
\[ m = \equiv tr^{-x} \equiv 193 \cdot 924 \equiv 21 \pmod{1213}. \]

(RSA.15) ElGamal Signature Scheme:

**Purpose** Send a message with an authentic signature (so that the receiver knows that it can be verified that the message is from the expected sender).

**Choosing System Parameters** A usually large prime \( p \), a primitive root \( a \mod p \).

**Making Enciphering and Deciphering Keys** Pick an integer \( e \) with \( 1 < e < p - 1 \) and compute \( b \equiv a^e \pmod{p} \). The encryption key \( E_K = (p, a, b) \). The number \( e \) is the secret decryption key.

Alice, who wants to sign her message to be sent to Bob, generates and publicists such an Enciphering key \( E_K = (p, a, b) \) while keeping \( e \) a secret. (Here we also use \( k = (p, a, e, b) \) to denote the system parameters).

**Signing Stage** Alice wants to sign a message \( m \in \mathbb{Z}^*_p \). She randomly chooses a number \( r \in \mathbb{Z}^*_{p-1} \) and computes \( h = a^r \pmod{p} \) and \( g = (m - eh)r^{-1} \pmod{p - 1} \). Alice then sends the message \( m \) together with the signed message \( \text{sig}_k(m, r) = (h, g) \).

**Verification Stage** Bob receives the message \( m \) and \( \text{sig}_k(m, r) = (h, g) \). Since Alice’s enciphering key \( K_E = (p, a, b) \) is in public domain, Bob downloads it and does the following:

(i) Computes \( h \equiv a^r \pmod{p} \). Bob accepts the signature if \( h \in \mathbb{Z}^*_p \), rejects it otherwise.

(ii) Computes \( d = b^h \cdot h^g \pmod{p} \) and \( s = a^m \pmod{p} \).

(iii) Bob considers the message is authentic if \( d \equiv s \pmod{p} \), and rejects it otherwise.

**Reason:** Note that \( eh + rg = eh + r(m - eh)r^{-1} = m \),
\[ d \equiv b^h \cdot h^g \equiv a^{eh} \cdot a^{rg} \equiv a^{eh + rg} \equiv a^m \equiv s \pmod{p}. \]

(RSA. 16A) **Example:** Bob receives \( \text{sig}_k(m, r) = (h, g) = (480, 532) \) together with \( m = 121 \) from Alice. Bob downloads Alice’s \( K_E = (p, a, b) = (641, 3, 88) \). Should Bob accepts it?

**Solution:** Bob recognizes that \( b = 88 \), \( h = 480 \), and \( g = 532 \). He computes
\[ d \equiv b^h \cdot h^g \equiv 88^{480} \cdot 480^{532} \equiv 191 \pmod{641}, \]
and
\[ s \equiv a^m \equiv 3^{121} \equiv 300 \pmod{641}. \]
As \( d \not\equiv s \pmod{641} \), Bob rejects it.

(RSA. 16B) **Example:** Bob receives \( \text{sig}_k(m, r) = (h, g) = (480, 21) \) together with \( m = 121 \) from Alice. Bob downloads Alice’s \( K_E = (p, a, b) = (641, 3, 88) \). Should Bob accepts it?
**Solution:** Bob recognizes that \( b = 88, \ h = 480, \) and \( g = 21. \) He computes
\[
d \equiv b^h \cdot h^g \equiv 88^{480} \cdot 480^{21} \equiv 300 \pmod{641},
\]
and
\[
s \equiv a^m \equiv 3^{121} \equiv 300 \pmod{641}.
\]
As \( d \equiv s \pmod{641}, \) Bob accepts it.