Algorithms and datastructures II

Lecture 13: Randomized agorithms and public cryptography

Jan Hubička

Department of Applied Mathematics
Charles University
Prague

Jan 4 2021

Randomized algorithms

1. Las Vegas Algorithms: always give correct result, gamble on speed
   - Quicksort with random choice of median
   - Quickselect with random choice of median
   - ...

Randomized algorithms

1. Las Vegas Algorithms: always give correct result, gamble on speed
    - Quicksort with random choice of median
    - Quickselect with random choice of median
    - . . .
2. Monte Carlo Algorithms: Deterministic speed, gamble on result
    - Estimate value of π.
    - . . .

Fermat's little theorem

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Proof.

Fermat's little theorem

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Proof.

1. Let a be a positive integer. Consider all strings of p symbols using alphabet with a different symbols. Total number of strings is a^p.

Fermat's little theorem

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Proof.

1. Let a be a positive integer. Consider all strings of p symbols using alphabet with a different symbols. Total number of strings is a^p.
2. Interpret strings as necklaces. String α is a friend of β if it differs only by rotation.

□

Fermat's little theorem

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Proof.

1. Let a be a positive integer. Consider all strings of p symbols using alphabet with a different symbols. Total number of strings is a^p.
2. Interpret strings as necklaces. String α is a friend of β if it differs only by rotation.

□

Example

The following are all strings of length 5 with 2 characters where each line is a necklace:

1. AAABB, AABBA, ABBAA, BBAAA, BAAAB,
2. AABAB, ABABA, BABAA, ABAAB, BAABA,
3. AABBB, ABBBA, BBBAA, BBAAB, BAABB,
4. ABABB, BABBA, ABBAB, BBABA, BABAB,
5. ABBBB, BBBBA, BBBAB, BBABB, BABBB,
6. BAAAA, AAAAB, AAABA, AABAA, ABAAA,
7. AAAAA,
8. BBBBB.

Clearly $32 - 2$ is divisible by 5.

Fermat's little theorem

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Proof.

1. Let a be a positive integer. Consider all strings of p symbols using alphabet with a different symbols. Total number of strings is a^p.
2. Interpret strings as necklaces. String α is a friend of β if it differs only by rotation.
3. If α has length p then it has either 1 friend if it consist of only one character and p friends otherwise.

□

Example

The following are all strings of length 5 with 2 characters where each line is a necklace:

1. `AAABB, AABBA, ABBAA, BBAAA, BAAAB,`
2. `AABAB, ABABA, BABAA, ABAAB, BAABA,`
3. `AABBB, ABBBA, BBBAA, BBAAB, BAABB,`
4. `ABABB, BABBA, ABBAB, BBABA, BABAB,`
5. `ABBBB, BBBBA, BBBAB, BBABB, BABBB,`
6. `BAAAA, AAAAB, AAABA, AABAA, ABAAA,`
7. `AAAAA,`
8. `BBBBB.`

Clearly $32 - 2$ is divisible by 5.

Fermat's little theorem

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Proof.

1. Let a be a positive integer. Consider all strings of p symbols using alphabet with a different symbols. Total number of strings is a^p.
2. Interpret strings as necklaces. String α is a friend of β if it differs only by rotation.
3. If α has length p then it has either 1 friend if it consist of only one character and p friends otherwise.
4. There are a strings with 1 friend and $a^p - a$ strings with a friends. Thus $a^p - a$ is divisible by p.

$\square$

Example

The following are all strings of length 5 with 2 characters where each line is a necklace:

1. AAABB, AABBA, ABBAA, BBAAA, BAAAB,
2. AABAB, ABABA, BABAA, ABAAB, BAABA,
3. AABBB, ABBBA, BBBAA, BBAAB, BAABB,
4. ABABB, BABBA, ABBAB, BBABA, BABAB,
5. ABBBB, BBBBA, BBBAB, BBABB, BABBB,
6. BAAAA, AAAAB, AAABA, AABAA, ABAAA,
7. AAAAA,
8. BBBBB.

Clearly $32 - 2$ is divisible by 5.

Fermat test

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

FermatTest (n, k)

1. Repeat k times:
2. $a \leftarrow$ random integer in range $[2, n-2]$.
3. If $a^{n-1} \neq 1 \mod n$: return "n is composite".
4. Return "n is probably prime".

Fermat test

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

FermatTest (n, k)

1. Repeat k times:
2. $a \leftarrow$ random integer in range $[2, n-2]$.
3. If $a^{n-1} \neq 1 \mod n$: return "n is composite".
4. Return "n is probably prime".

Observation

If n is prime, then FermatTest will return "n is probably prime".

Fermat test

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

FermatTest (n, k)

1. Repeat k times:
2. $a \leftarrow$ random integer in range $[2, n-2]$.
3. If $a^{n-1} \neq 1 \mod n$: return "n is composite".
4. Return "n is probably prime".

If n is composite and a satisfies $a^{n-1} = 1 \mod n$, then a is called Fermat liar.

Fermat test

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

FermatTest (n, k)

1. Repeat k times:
2. $a \leftarrow$ random integer in range $[2, n-2]$.
3. If $a^{n-1} \neq 1 \mod n$: return "n is composite".
4. Return "n is probably prime".

If n is composite and a satisfies $a^{n-1} = 1 \mod n$, then a is called Fermat liar.

Definition

n is Carmichael numbers if all values a satisfying $gcd(a, n) = 1$ are Fermat liars. $561 = 3 \cdot 11 \cdot 17$

Fermat test

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

FermatTest (n, k)

1. Repeat k times:
2. $a \leftarrow$ random integer in range $[2, n-2]$.
3. If $a^{n-1} \neq 1 \mod n$: return "n is composite".
4. Return "n is probably prime".

If n is composite and a satisfies $a^{n-1} = 1 \mod n$, then a is called Fermat liar.

Definition

n is Carmichael numbers if all values a satisfying $gcd(a, n) = 1$ are Fermat liars. $561 = 3 \cdot 11 \cdot 17$

Fact (Bad news)

There are infinitely many Carmichael numbers.

For Carmichael number Fermant test performs poorly — it only return "n is composite" if the randomly chosen value a divides n.

Rabin-Miller primality test

RabinMiller (n, k)

Decompose n as $2^r d + 1$ with d odd.
repeat k times:
    $a \leftarrow$ random integer in range $[2, n-2]$.
    $x \leftarrow a^d \mod n$.
    if $x = 1$ or $x = n - 1$: continue outer loop.
    repeat $r - 1$ times:
        $x \leftarrow x^2 \mod n$.
        if $x = n - 1$: continue outer loop.
    return "n is composite".
return "n is probably prime".

Rabin-Miller primality test

RabinMiller (n, k)

Decompose n as $2^r d + 1$ with d odd.
repeat k times:
    $a \leftarrow$ random integer in range $[2, n-2]$.
    $x \leftarrow a^d \mod n$.
    if $x = 1$ or $x = n - 1$: continue outer loop.
    repeat $r - 1$ times:
        $x \leftarrow x^2 \mod n$.
        if $x = n - 1$: continue outer loop.
    return "n is composite".
return "n is probably prime".

Running time: $O(k \log^3 n)$

Rabin-Miller primality test

RabinMiller (n, k)

1. Decompose n as $2^r d + 1$ with d odd.
2. repeat k times:
3. $\quad a \leftarrow$ random integer in range $[2, n-2]$.
4. $\quad x \leftarrow a^d \mod n$.
5. $\quad$ if $x = 1$ or $x = n - 1$: continue outer loop.
6. $\quad$ repeat $r - 1$ times:
7. $\quad\quad x \leftarrow x^2 \mod n$.
8. $\quad\quad$ if $x = n - 1$: continue outer loop.
9. $\quad$ return "n is composite".
10. return "n is probably prime".

Running time: $O(k \log^3 n)$

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if $a^d = 1 \mod n$ and $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Observation

The only square roots of 1 modulo p are 1 and -1.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Observation

The only square roots of 1 modulo p are 1 and -1.

Proof.

Clearly $1^2 = (-1)^2 = 1$.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Observation

The only square roots of 1 modulo p are 1 and -1.

Proof.

Clearly $1^2 = (-1)^2 = 1$. Consider polynomial $X^2 - 1 = 0 \mod n$. this is a polynomial of degree 2 and thus has 2 roots (over a finite field). □

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Observation

The only square roots of 1 modulo p are 1 and -1.

Theorem

Every odd prime n is also strong probable prime to base a for every valid choice of a.

Each term of sequence $a^{2^r d}, a^{2^{r-1}} d, \ldots, a^d$ is a square root of previous.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Observation

The only square roots of 1 modulo p are 1 and -1.

Theorem

Every odd prime n is also strong probable prime to base a for every valid choice of a.

Each term of sequence $a^{2^r d}, a^{2^{r-1}} d, \dots, a^d$ is a square root of previous. We have $a^{2^r d} = 1 \mod p$.

Strong probable primes

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

Theorem (Fermat's little theorem)

Given prime number p, integer a then $a^p = a \mod p$.

Observation

The only square roots of 1 modulo p are 1 and -1.

Theorem

Every odd prime n is also strong probable prime to base a for every valid choice of a.

Each term of sequence $a^{2^r d}, a^{2^{r-1}} d, \ldots, a^d$ is a square root of previous. We have $a^{2^r d} = 1 \mod p$.
It follows that second term is either 1 or -1. If it is -1 we are done. Otherwise repeat argument.

Accuracy of Rabin-Miller primality test

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

We call a strong liar for n if n is composite and n is strong probable prime to base a.

Accuracy of Rabin-Miller primality test

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

We call a strong liar for n if n is composite and n is strong probable prime to base a.

Fact

If n is composite then at most $1/4$ bases a are strong liars.

Accuracy of Rabin-Miller primality test

Definition (Strong probable prime)

Given an odd integer $n = 2^r d + 1$ where r is a positive integer and d is an odd positive integer and $0 < a < n$ we say that n is strong probable prime to base a if

1. $a^d = 1 \mod n$ and
2. $a^{2^s d} = -1 \mod n$ for some $0 \leq s \leq r$.

We call a strong liar for n if n is composite and n is strong probable prime to base a.

Fact

If n is composite then at most $1/4$ bases a are strong liars.

Corollary

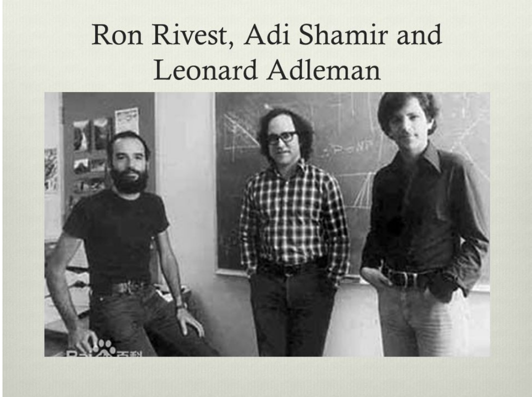
if n is composite then running k iterations of the Miller–Rabin test will declare n probably prime with a probability at most 4^{-k}.

Public key cryptography

Suppose that Alice and Bob wants to send private messages over a public channel.

Public key cryptography

Suppose that Alice and Bob wants to send private messages over a public channel.



Public key cryptography

Suppose that Alice and Bob wants to send private messages over a public channel.

RSA (1978)

RSA (Rivest–Shamir–Adleman) consists of 3 steps:

1. Key generation
2. Key distribution
3. Encryption
4. Decryption

Public key cryptography

Suppose that Alice and Bob wants to send private messages over a public channel.

RSA (1978)

RSA (Rivest–Shamir–Adleman) consists of 3 steps:

1. Key generation
2. Key distribution
3. Encryption
4. Decryption

Basic principle

We can find very large integers e, d and n such that

$$(m^e)^d = m \mod n.$$

For every $0 \leq m < n$. Knowing e, n and m it is hard to find d.

Public key cryptography

Suppose that Alice and Bob wants to send private messages over a public channel.

RSA (1978)

RSA (Rivest–Shamir–Adleman) consists of 3 steps:

1. Key generation
2. Key distribution
3. Encryption
4. Decryption

Basic principle

We can find very large integers e, d and n such that

$$(m^e)^d = m \mod n.$$

For every $0 \leq m < n$. Knowing e, n and m it is hard to find d.
We can also exchange exponents:

$$(m^d)^e = m \mod n.$$

RSA

Key generation

1. Choose distinct prime numbers p and q.
   (p and q are kept secret and can be found using Rabin-Miller test)

RSA

Key generation

1. Choose distinct prime numbers p and q.
   (p and q are kept secret and can be found using Rabin-Miller test)
2. $n \leftarrow pq$.
   (n is the modulus and released as a public key)

RSA

Key generation

1. Choose distinct prime numbers p and q.
   (p and q are kept secret and can be found using Rabin-Miller test)
2. $n \leftarrow pq$.
   (n is the modulus and released as a public key)
3. Compute $\lambda(n) = lcm(p-1, q-1)$.
   (λ is Carmichael's totient function: $\lambda(n)$ is the minimal number m satisfying $a^m = 1 \mod n$ for all $0 \leq a \leq n$ such that a is coprime to n: $gcd(a, n) = 1$)

RSA

Key generation

1. Choose distinct prime numbers p and q.
   (p and q are kept secret and can be found using Rabin-Miller test)
2. $n \leftarrow pq$.
   (n is the modulus and released as a public key)
3. Compute $\lambda(n) = lcm(p-1, q-1)$.
   (λ is Carmichael's totient function: $\lambda(n)$ is the minimal number m satisfying $a^m = 1 \mod n$ for all $0 \leq a \leq n$ such that a is coprime to n: $gcd(a, n) = 1$)
4. Choose e such that $1 \leq e \leq \lambda(n)$ and e is coprime to $\lambda(n)$.
   (e is released as part of public key.)

RSA

Key generation

1. Choose distinct prime numbers p and q.
   (p and q are kept secret and can be found using Rabin-Miller test)
2. $n \leftarrow pq$.
   (n is the modulus and released as a public key)
3. Compute $\lambda(n) = lcm(p-1, q-1)$.
   (λ is Carmichael's totient function: $\lambda(n)$ is the minimal number m satisfying $a^m = 1 \mod n$ for all $0 \leq a \leq n$ such that a is coprime to n: $gcd(a, n) = 1$)
4. Choose e such that $1 \leq e \leq \lambda(n)$ and e is coprime to $\lambda(n)$.
   (e is released as part of public key.)
5. Determine $d = e^{-1} \mod \lambda(n)$ using extended Euclidean algorithm.
   (d is kept secret)

RSA

Key generation

1. Choose distinct prime numbers p and q.
   (p and q are kept secret and can be found using Rabin-Miller test)
2. $n \leftarrow pq$.
   (n is the modulus and released as a public key)
3. Compute $\lambda(n) = lcm(p-1, q-1)$.
   (λ is Carmichael's totient function: $\lambda(n)$ is the minimal number m satisfying $a^m = 1 \mod n$ for all $0 \leq a \leq n$ such that a is coprime to n: $gcd(a, n) = 1$)
4. Choose e such that $1 \leq e \leq \lambda(n)$ and e is coprime to $\lambda(n)$.
   (e is released as part of public key.)
5. Determine $d = e^{-1} \mod \lambda(n)$ using extended Euclidean algorithm.
   (d is kept secret)

Key distribution

Alice will generate key and communicate (n, e) via reliable (not necessarily secret) route.

RSA

Encryption

Bob chooses a message m (an integer satisfying $0 \leq m < n$) and computes

$$c = m^e \mod n$$

and transmits c to Alice.

Decryption

Alice computes

$$c^d = (m^e)^d = m \mod n$$

Example and correctness

1. Choose two distinct prime numbers p and q.
(Such as $p = 61$ and $q = 53$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p - 1, q - 1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)
7. The private key is ($n = 3233$, $d = 413$).
   Decryption is: $m(c) = c^{413} \mod 3233$.
   ($c = 2790$, $m = 2790^{413} \mod 3233 = 65$.)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)
7. The private key is ($n = 3233$, $d = 413$).
   Decryption is: $m(c) = c^{413} \mod 3233$.
   ($c = 2790$, $m = 2790^{413} \mod 3233 = 65$.)

Theorem

$(m^e)^d = m \mod pq$

Proof.

Since $\lambda(pq) = lcm(p-1, q-1)$ is divisible by $p-1$ and $q-1$ we have

$$ed - 1 = h(p-1) = k(q-1)$$

for some h and q.

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)
7. The private key is ($n = 3233$, $d = 413$).
   Decryption is: $m(c) = c^{413} \mod 3233$.
   ($c = 2790$, $m = 2790^{413} \mod 3233 = 65$.)

Theorem

$(m^e)^d = m \mod pq$

Proof.

Since $\lambda(pq) = lcm(p-1, q-1)$ is divisible by $p-1$ and $q-1$ we have

$$ed - 1 = h(p-1) = k(q-1)$$

for some h and q.
We show that $m^{ed} = m \mod p$. Consider two cases

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)
7. The private key is ($n = 3233$, $d = 413$).
   Decryption is: $m(c) = c^{413} \mod 3233$.
   ($c = 2790$, $m = 2790^{413} \mod 3233 = 65$.)

Theorem

$(m^e)^d = m \mod pq$

Proof.

Since $\lambda(pq) = lcm(p-1, q-1)$ is divisible by $p-1$ and $q-1$ we have

$$ed - 1 = h(p-1) = k(q-1)$$

for some h and q.
We show that $m^{ed} = m \mod p$. Consider two cases

1. $m = 0 \mod p$: then m^{ed} is a multiple of p and $m^{ed} = 0 = m \mod p$.

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)
7. The private key is ($n = 3233$, $d = 413$).
   Decryption is: $m(c) = c^{413} \mod 3233$.
   ($c = 2790$, $m = 2790^{413} \mod 3233 = 65$.)

Theorem

$(m^e)^d = m \mod pq$

Proof.

Since $\lambda(pq) = lcm(p-1, q-1)$ is divisible by $p-1$ and $q-1$ we have

$$ed - 1 = h(p-1) = k(q-1)$$

for some h and q.
We show that $m^{ed} = m \mod p$. Consider two cases

1. $m = 0 \mod p$: then m^{ed} is a multiple of p and $m^{ed} = 0 = m \mod p$.
2. $m \neq 0 \mod p$: $m^{ed} = m^{ed-1}m = m^{h(p-1)}m = (m^{p-1})^h m = 1^h m = m \mod p$
   (By Fermat little theorem $m^{p-1} = 1 \mod p$)

Example and correctness

1. Choose two distinct prime numbers p and q.
   (Such as $p = 61$ and $q = 53$.)
2. Compute $n = pq$.
   ($n = 61 \cdot 53 = 3233$.)
3. Compute the Carmichael's totient function of the product as $\lambda(n) = lcm(p-1, q-1)$.
   ($\lambda(3233) = lcm(60, 52) = 78$.)
4. Choose any number $1 < e < 780$ that is coprime to 780.
   (Let $e = 17$.)
5. Compute d, the modular multiplicative inverse of e modulo $\lambda(n)$.
   ($d = 413$ as $1 = (17 \cdot 413) \mod 780$.)
6. The public key is ($n = 3233$, $e = 17$).
   Encryption is: $c(m) = m^{17} \mod 3233$.
   (put $m = 65$, $c = 65^{17} \mod 3233 = 2790$.)
7. The private key is ($n = 3233$, $d = 413$).
   Decryption is: $m(c) = c^{413} \mod 3233$.
   ($c = 2790$, $m = 2790^{413} \mod 3233 = 65$.)

Theorem

$(m^e)^d = m \mod pq$

Proof.

Since $\lambda(pq) = lcm(p-1, q-1)$ is divisible by $p-1$ and $q-1$ we have

$$ed - 1 = h(p-1) = k(q-1)$$

for some h and q.
We show that $m^{ed} = m \mod p$. Consider two cases

1. $m = 0 \mod p$: then m^{ed} is a multiple of p and $m^{ed} = 0 = m \mod p$.
2. $m \neq 0 \mod p$: $m^{ed} = m^{ed-1}m = m^{h(p-1)}m = (m^{p-1})^h m = 1^h m = m \mod p$
   (By Fermat little theorem $m^{p-1} = 1 \mod p$)

Analogously $m^{ed} = m \mod q$ and thus $m^{ed} = m \mod pq$ □

Thank you