1 Modular Exponention Function

An integer g is a primitive root modulo n if every integer a coprime to n is congruent to a power of g modulo n. For every integer a coprime to n, there exists an integer k such that $a = g^k \bmod n$. In other words, g is the generator of a multiplicative group modulo $n :< g >= U(n) = \mathbb{Z}_n^\times$. It is also called a primitive element in $U(n)$.

Example 1. 3 is a primitive root modulo 7, since

$$< 3 >= \{3, 2, 6, 4, 5, 1\} = U(7) \ .$$

Group $U(n)$ is cyclic iff $n \in \{2, 4, p^k, 2p^k\}$, where p^k is some power of an odd prime number p.

Example 2. Find primitive elements in $\mathbb{Z}_{14}^\times$.

Solution. $\mathbb{Z}_{14}^\times = \{1, 3, 5, 9, 11, 13\}$.

$$\begin{aligned}
\langle 3 \rangle &= \{3, 9, 13, 11, 5, 1\} \\
\langle 5 \rangle &= \{5, 11, 13, 9, 3, 1\} \\
\langle 9 \rangle &= \{9, 11, 1\} \\
\langle 11 \rangle &= \{11, 9, 1\} \\
\langle 13 \rangle &= \{13, 1\}
\end{aligned}$$

The primitive elements are 3 and 5, since $\mathbb{Z}_{14}^\times = \langle 3 \rangle = \langle 5 \rangle$.

Example 3. Verify if 2 and 3 are primitive roots modulo 11.

Solution. Since a primitive root modulo 11 generates $U(11)$, the order of a generator is $\varphi(11) = 10$. Observe that

$$\begin{aligned}
\langle 2 \rangle &= \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = U(11) \\
\langle 3 \rangle &= \{3, 9, 5, 4, 1\} \neq U(11)
\end{aligned}$$

It can be seen that $\operatorname{ord} 2 = 10$ and $\operatorname{ord} 3 = 5$. Hence, 2 is a primitive root modulo 11, while 3 is not.

No simple general formula for computing primitive roots modulo n is known. The number of primitive roots modulo n (if there are any), is equal to $\varphi(\varphi(n))$, since in general a cyclic group of order r has $\varphi(r)$ generators.

2 Diffie-Hellman Key Establishment

2.1 Key Establishment Protocol

Alice and Bob agree on common parameters – a cyclic group $\mathcal{G}$, its generator $g \in \mathcal{G}$, its order $|\mathcal{G}| = q$. Alice selects $x \in \mathbb{Z}_q$ and sends g^x to Bob. Bob selects $y \in \mathbb{Z}_q$ and sends g^y to Alice. Alice computes $g^{xy} = (g^y)^x \in \mathcal{G}$. Bob computes $g^{xy} = (g^x)^y \in \mathcal{G}$.

2.2 MITM Attack Against DH

Alice and Bob agree on common parameters – a cyclic group $\mathcal{G}$, its generator $g \in \mathcal{G}$, its order $|\mathcal{G}| = q$. Alice selects $x \in \mathbb{Z}_q$ and sends g^x to Bob, but Carol intercepts this message. She generates $z \in \mathbb{Z}_q$, and impersonating Alice sends g^z to Bob. Bob selects $y \in \mathbb{Z}_q$ and sends g^y to Alice. Carol intercepts this message, and impersonating Bob, sends g^z to Alice. Alice computes $g^{xz} = (g^z)^x \in \mathcal{G}$. Bob computes $g^{yz} = (g^z)^y \in \mathcal{G}$. Carol computes $g^{xz} = (g^x)^z \in \mathcal{G}$, and $g^{yz} = (g^y)^z \in \mathcal{G}$.

3 $\mathcal{O}$- and o- notations

The assertion $f(n) = \mathcal{O}(g(n))$ if for sufficiently large values of n, the value of $f(n)$ is at most a positive constant multiple of $g(n)$.

$$f(n) = \mathcal{O}(g(n)) \iff \exists k \in \mathbb{R}, k > 0, \exists n_0 \in \mathbb{R} \forall n \in \mathbb{R}, n > n_0 : f(n) \leqslant k \cdot g(n) \ .$$

This means that

$$\limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty \ .$$

Example 4. Show that $3n^3 + 2n^2 = \mathcal{O}(n^3)$.

Solution.

$$\limsup_{n\to\infty} \frac{3n^3 + 2n^2}{n^3} = \limsup_{n\to\infty} 3 + \frac{2}{n} = 3 < \infty \ .$$

The assertion $f(n) = o(g(n))$ intuitively means that $g(n)$ grows much faster than $f(n)$.

$$f(n) = o(g(n)) \iff \forall \varepsilon \in \mathbb{R}, \varepsilon > 0, \exists n_0 \in \mathbb{R} \forall n \in \mathbb{R}, n > n_0 : f(n) < \varepsilon \cdot g(n) \ .$$

This means that

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0 \ .$$

Example 5. Show that $n^2 \neq o(n)$.

Solution. There exists $k = 5$ and $n_0 = 1$ such that for all $n > 1$ it holds that $3n^3 + 2n^2 \leqslant 5n^3$.

$$\lim_{n\to\infty} \frac{n^2}{n} = \lim_{n\to\infty} = \infty \neq 0 \ .$$

Example 6. Show that $n^2 = o(n^3)$.

Solution. There exists $n_0 = 0$ such that for all $n > n_0$ and for every arbitrarily small value ε it holds that $n^2 < \varepsilon \cdot n^3$.

$$\lim n \to \infty \frac{n^2}{n^3} = \lim n \to \infty \frac{1}{n} = 0 \ .$$

4 The notion of S-security and security bits

Definition 1. A problem P is S-secure against attack X if every adversary A that uses t time units has success

$$\delta \leqslant \frac{t}{S} \ ,$$

where t is the time measured in block cipher units, and S is the left-cost of P (also measured in block cipher units).

In other words, for all adversaries A with running time t it holds that

$$\frac{t}{\delta} \geqslant S \ .$$

The value t/δ is called the adversarial cost–success ratio. It turns out that not t nor δ determine the self-cost of P, but their ratio, the cost–success ratio.

5 RSA setup

Example 7. Given prime numbers p and q, find suitable public and private exponents.

Solution. Given p and q, they determine $n = pq$. Also $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ is known. Public exponent e and private exponent d are tied together by the following relation $ed \equiv 1 \pmod{\varphi(n)}$. Hence e and d must be invertible elements modulo $\varphi(n)$. It means that $\gcd(\varphi(n), e) = \gcd((p-1)(q-1), e) = 1 \implies \gcd(p-1, e) = \gcd(q-1, e) = 1$. Then $d = e^{-1} \pmod{\varphi(n)}$.

Example 8. Given a public exponent, find suitable prime numbers.

Solution. Public exponent e must be invertible modulo $\varphi(n)$, and the primes p and q determine n. Suitable prime numbers p and q are the ones such that $\gcd(p-1, e) = \gcd(q-1, e) = 1$.

Example 9. Given a public exponent, determine if given primes are OK for RSA.

Solution. Given a public exponent e and primes p and q, we need to check if $\gcd(p-1, e) = \gcd(q-1, e) = 1$.

6 Probabilistic Prime Number Tests

Example 10. Given the required reliability of the test, calculate number of trials.

Solution. If n runs of the probabilistic prime number test (such as Fermat test or Miller-Rabin test) succeeded, then the probability that a given integer is prime is $1 - 2^{-n}$. If the reliability of the test is required, i.e. the probability must be at least p, then we obtain inequality $p \leqslant 1 - 2^{-n}$ or $2^{-n} \leqslant 1 - p$. Taking $\log_2$ on both sides gives us $n \geqslant -\log_2(1-p)$.

Example 11. How many iterations of probabilistic primality test do we need to make to reach confidence at least 0.999?

Solution. It can be seen that

$$0.999 \leqslant 1 - 2^{-n} \implies 2^{-n} \leqslant 0.001 \implies \log_2 2^{-n} \leqslant log_2 0.001 \implies -n \leqslant -9.96 \implies n \geqslant 9.96 \ .$$

The smallest such integer is $n = 10$. Indeed, $1 - 2^{-10} = \frac{1023}{1024} \approx 0.9990234375$.

7 Common Modulus RSA

Suppose the same message m was encrypted to two people with private keys (e_1, n) and (e_2, n), with $e_1 \neq e_2$. If $\gcd(e_1, e_2) = 1$, then by the Bézout identity there exist integers $\alpha, \beta \in \mathbb{Z}$ such that $\alpha e_1 + \beta e_2 = 1$. Then the attacker can exploit this identity to recover message m as

$$(m^{e_1})^{\alpha} \bmod n \cdot (m^{e_2})^{\beta} \bmod n = m^{\alpha e_1 + \beta e_2} \bmod n = m \bmod n \ .$$

Example 12. Suppose the cryptogram $c_1 = 537$ was encrypted with public key $(e = 18, n = 943)$ and the cryptogram $c_2 = 285$ was encrypted with public key $(e = 19, n = 943)$, and the same message m was encrypted, then

$$\gcd(18, 19) = 1 = 1 \cdot 19 + (-1) \cdot 18$$
$$537^{-1} \cdot 285 \bmod 943 = 72 \cdot 285 \bmod 943 = 717 \bmod 943 \ .$$

8 Chinese Remainder Theorem

Example 13. Solve for x:

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 11 \pmod{13} \end{cases}$$

Solution.

$$\gcd(12, 13) = 1 = (-1) \cdot 12 + 1 \cdot 13$$
$$x = -11 \cdot 12 + 7 \cdot 13 = 91 - 132 = -41 \equiv 115 \pmod{156}$$

Example 14. Solve for x:

$$\begin{cases} x \equiv 11 \pmod{25} \\ x \equiv 14 \pmod{19} \\ x \equiv 13 \pmod{17} \end{cases}$$

Solution.

$N = 25 \cdot 19 \cdot 17 = 8075$

$N_1 = \dfrac{8075}{25} = 323 \ , \quad \gcd(25, 323) = 1 = (-155) \cdot 25 + 12 \cdot 323$

$N_2 = \dfrac{8075}{19} = 425 \ , \quad \gcd(19, 425) = 1 = 179 \cdot 19 + (-8) \cdot 425$

$N_3 = \dfrac{8075}{17} = 475 \ , \quad \gcd(17, 475) = 1 = 28 \cdot 17 + (-1) \cdot 475$

$x = 11 \cdot 12 \cdot 323 + 14 \cdot (-8) \cdot 425 + 13 \cdot (-1) \cdot 475 = 42636 - 47600 - 6175 = -11139 \equiv 5011 \pmod{8075}$

$5011 \equiv 11 \pmod{25} \ , \quad 5011 \equiv 14 \pmod{19} \ , \quad 5011 \equiv 13 \pmod{17}$

9 Finding Nontrivial Square Roots of 1

If the prime factorization of n is $n = p_1^{e_1} \cdots p_k^{e_k}$, then $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{e_1}}^\times \times \ldots \times \mathbb{Z}_{p_k^{e_k}}^\times$. Each group $Z_{p_i^{e_i}}^\times$ is a cyclic prime order group, there are exactly two trivial roots of unity, 1 and $p_k^{e_k} - 1$, and no nontrivial roots, and the total amount of roots of unity in $\mathbb{Z}_n^\times$ is $2k$, where 2 of them are trivial and $2k - 1$ are nontrivial.

Example 15. Find nontrivial roots of unity in $\mathbb{Z}_{315}^\times$, given that $315 = 3^2 \cdot 5 \cdot 7$.

Solution. It is known that $\mathbb{Z}_{315}^\times \cong \mathbb{Z}_9^\times \times \mathbb{Z}_5^\times \times \mathbb{Z}_7^\times$. Group $\mathbb{Z}_9^\times$ has two nontrivial roots of unity 1 and 8, the roots of unity in $\mathbb{Z}_5^\times$ are 1 and 4, and the roots of unity in $\mathbb{Z}_7^\times$ are 1 and 6. Hence, $\mathbb{Z}_{315}^\times$ has 8 roots of unity in total – 2 trivial and 6 nontrivial. Consider the mapping $\psi : \mathbb{Z}_9^\times \times \mathbb{Z}_5^\times \times \mathbb{Z}_7^\times \to \mathbb{Z}_{315}^\times$:

$$
\begin{aligned}
(1,1,1) &\mapsto 1 & (8,1,1) &\mapsto 71 \\
(1,1,6) &\mapsto 181 & (8,1,6) &\mapsto 251 \\
(1,4,1) &\mapsto 64 & (8,4,1) &\mapsto 134 \\
(1,4,6) &\mapsto 244 & (8,4,6) &\mapsto 314
\end{aligned}
$$

Suppose you learn that $a^k \equiv 1 \pmod{n}$. If k is even, it is a multiple of 2. If we express k in the form $k = 2^s \cdot d$, then we can apply the Miller-Rabin algorithm to find the nontrivial square root of 1 modulo n.

Example 16. Suppose you are looking for nontrivial square roots of 1 modulo 2491, and you have learned that $7^{4784} \equiv 1 \pmod{2)491}$. You can express 4784 as $2^4 \cdot 299$ and apply the Miller-Rabin algorithm as follows

$$
\begin{aligned}
7^{299} \bmod 2491 &= 847 \\
847^2 \bmod 2491 &= 1
\end{aligned}
$$

Square roots of 1 modulo n can be found using the Miller–Rabin algorithm, if we manage to find base a for which n is a probable prime to

1. n is a probable prime to base a
2. n is a strong pseudoprime to base a

Exercise 1. Suppose you have found a base 187 for which 1457 is a probable prime and a strong pseudoprime. $1456 = 2^4 \cdot 91$.

$$
\begin{aligned}
187^{91} \bmod 1457 &= 187 \\
187^2 \bmod 1457 &= 1
\end{aligned}
$$

Hence, 187 is a nontrivial square root of 1 modulo 1457.

10 Factoring with Nontrivial Square Roots of 1 modulo n

If n is a product of two primes and a is a nontrivial square root of 1 modulo n, such that $a^2 \equiv 1 \pmod{n}$, then the factors of n can be obtained by calculating $\gcd(a-1, n)$ and $\gcd(a+1, n)$.

Example 17. Consider $n = 221$, and a nontrivial square root of 1 is 103, meaning that $103^2 \equiv 1 \pmod{221}$. The goal is to factor 221 into two distinct primes p and q.

Solution.

$$p = \gcd(102, 221) = 17$$
$$q = \gcd(104, 221) = 13$$

Hence, $221 = 13 \cdot 17$.

11 Small Public Modulus Attack Against Pure RSA

Example 18. Suppose the same message was encrypted with public keys $(e = 3, n = 377), (e = 3, n = 391), (e = 3, n = 589)$. The three cryptograms are $330, 34, 419$. Find m.

Solution. The solution to the CRT

$$C \equiv 330 \pmod{377}$$
$$C \equiv 34 \pmod{391}$$
$$C \equiv 419 \pmod{589}$$

is 1061208 mod 86822723, which is m^3. Taking cubic root of it reveals the message

$$\sqrt[3]{1061208} = 102 \ .$$

12 Blind Signatures and Chaum's Digital Cash

A form of digital signature in which the content of a message is blinded before it is signed, so that the signer never sees the message. The resulting signature can be verified against the original message as a regular digital signature.

Blind signature schemes exist for many public key signing protocols. One of the simplest blind signature schemes is based on RSA.

The message author generates a random blinding factor $r \in \mathbb{Z}^{\times}_{\varphi(n)}$ with $\gcd(r, n) = 1$. The value $r^e \bmod n$ is used as the blinding factor. The message author submits $m' = m \cdot r^e \bmod n$ to the signing authority, who signs m', and the blinded signature is $s' = (m')^d \bmod n$. This signature is sent back to the author, who removes the blinding factor to obtain the signature $s \equiv s' \cdot r^{-1} \pmod{n}$ on the original message. It can be seen that

$$s \equiv s' \cdot r^{-1} \pmod{n} \implies (m \cdot r^e \bmod n)^d \cdot r^{-1} \bmod n = m^d \cdot r^{ed} \cdot r^{-1} \bmod n = m^d \bmod n \ .$$

The signature s can be verified as any other RSA signature: $s^e \bmod n = m^{ed} \bmod n = m$.

For Chaum's digital cash read `https://www.win.tue.nl/~berry/papers/cosic.pdf`.

Homomorphic properties of RSA can be used to attack coins and make a third coin out of existing two. Let the first coin be $c_1^d \bmod n$, and the second coin be $c_2^d \bmod n$. Due to the homomorphic properties of plain RSA, the product of signatures is a signature of the product. Hence,

$$c_1^d \bmod n \cdot c_2^d \bmod n = (c_1 \cdot c_2)^d \bmod n \ .$$

13 Homomorphic Properties of RSA

A mapping $\varphi : (G, \cdot) \to (H, \bullet)$ is a homomorphism if φ is injective and the group operation is preserved

$$\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) \bullet \varphi(b) \ .$$

RSA is homomorphic w.r.t multiplication – the product of two cryptograms is the encrypted product of two plaintexts, and the encryption function is homomorphism. Let the encryption function be E. Then

$$E(m_1 \cdot m_2) = E(m_1) \cdot E(m_2) \ ,$$

where $\cdot$ is the multiplication operation. Homomorphic cryptosystems are not IND-CCA2 secure (not secure against adaptive chosen ciphertext attacks). It can be shown that plain RSA is not IND-CCA2 secure by demonstrating that there exists an adversary which can always win the IND-CCA2 game. When such an adversary receives the challenge cryptogram from the challenger, it uses an encryption oracle to compose his own crafted cryptogram containing some blinding factor as the message, then submits the product of this cryptogram and the challenge cryptogram to the decryption oracle, thus obtaining the product of the original message and the blinding factor. All such an adversary needs to do is to divide the result by the blinding factor to reveal the message. Using this procedure, an adversary can always win the IND-CCA2 game.