In An RSA System, The Public Key Of A Given User Is E = 31, N = 3599. What Is The Private Key Of This

In An RSA System, The Public Key Of A Given User Is E = 31, N = 3599. What Is The Private Key Of This?

RSA (Rivest-Shamir-Adleman) is one of the most widely used public key cryptographic systems. Its security hinges on the mathematical difficulty of factoring large composite numbers. In this article, we will explore how to determine the private key, specifically the private exponent d, given a public key (E, N). The process involves understanding the core principles of RSA, factoring the modulus N, computing Euler's totient function $\phi(N)$, and deriving the modular inverse of the public exponent E modulo $\phi(N)$.

Understanding the RSA Public and Private Keys

Components of RSA Keys

The RSA cryptosystem involves two keys:

- **Public Key**: Composed of the exponent E and modulus N, publicly shared for encryption.
- **Private Key**: Composed of the exponent D (often denoted as d) and the same modulus N, kept secret for decryption.

The key relationship:

$$
E \times D \equiv 1 \pmod{\phi(N)}
$$

where $\phi(N)$ is Euler's totient function of N.

Given Data

- Public exponent: $E = 31$
- Modulus: $N = 3599$

Our goal is to determine the private exponent D.

Step 1: Factor the Modulus N

Understanding the Importance of Factoring N

To find $\phi(N)$, we need to factor N into its prime components:
$$
N = p \times q
$$
where p and q are prime numbers.

Factoring 3599

Let's attempt to factor 3599:

- Check small primes:
- 2: 3599 is odd, so no.
- 3: Sum of digits = 3 + 5 + 9 + 9 = 26, not divisible by 3.
- 5: Last digit not 0 or 5, so no.
- 7: 7 514 = 3598, close but 3599 - 3598 = 1, so no.
- 11: 3 - 5 + 9 - 9 = -2, not divisible by 11.
- 13: 13 277 = 3601, too high.
- 17: 17 211 = 3587, close but no.
- 19: 19 189 = 3591, close but no.
- 23: 23 156 = 3588, no.
- 29: 29 124 = 3596, no.
- 31: 31 116 = 3596, no.
- 37: 37 97 = 3589, no.
- 41: 41 87 = 3567, no.
- 43: 43 83 = 3589, no.
- 47: 47 76 = 3572, no.
- 53: 53 67 = 3551, no.
- 59: 59 61 = 3599. Bingo!

Thus:
$$
N = 3599 = 59 \times 61
$$

Both 59 and 61 are prime numbers.

Step 2: Compute Euler's Totient $\phi(N)$

For two distinct primes p and q:
$$
\phi(N) = (p - 1)(q - 1)
$$

Calculate:
$$
\phi(3599) = (59 - 1) \times (61 - 1) = 58 \times 60 = 3480
$$

Step 3: Find the Modular Inverse of E mod $\phi(N)$

We need to find D such that:
$$
E \times D \equiv 1 \pmod{3480}
$$
or
$$
31 \times D \equiv 1 \pmod{3480}
$$

This is a modular inverse problem.

Using Extended Euclidean Algorithm

The Extended Euclidean Algorithm finds integers x and y satisfying:
$$
ax + by = \gcd(a, b)
$$
If $\gcd(a, b) = 1$, then x is the modular inverse of a modulo b.

Set:
$$
a = 31, \quad b = 3480
$$

Perform the algorithm:

1. Divide 3480 by 31:
$$
3480 = 31 \times 112 + 8
$$
2. Divide 31 by 8:
$$
31 = 8 \times 3 + 7
$$
3. Divide 8 by 7:
$$
8 = 7 \times 1 + 1
$$
4. Divide 7 by 1:

$$
7 = 1 \times 7 + 0
$$

Back-substitute to express 1 as a combination of 31 and 3480:

- $1 = 8 - 7 \times 1$
- But $7 = 31 - 8 \times 3$, so:
$$
1 = 8 - (31 - 8 \times 3) \times 1 = 8 - 31 + 8 \times 3 = 8 \times 4 - 31
$$
- And $8 = 3480 - 31 \times 112$, so:
$$
1 = (3480 - 31 \times 112) \times 4 - 31
$$
$$
1 = 3480 \times 4 - 31 \times 448 - 31 = 3480 \times 4 - 31 \times 449
$$

Thus:
$$
1 \equiv -449 \times 31 \pmod{3480}
$$

The modular inverse D is the value of x such that:
$$
31 \times x \equiv 1 \pmod{3480}
$$

From above:
$$
x \equiv -449 \pmod{3480}
$$
which is equivalent to:
$$
x \equiv 3480 - 449 = 3031
$$

Since D must be positive and less than $\phi(N)$, we have:
$$
D = 3031
$$

Step 4: Confirm the Private Key

The private key exponent D is:
$$
\boxed{
D = 3031
```
```

}
\]

Thus, the private key corresponding to the public key \((E=31, N=3599) \) is:

\[
\boxed{
\text{Private Key } D = 3031
}
\]

and the complete private key pair is:
\[
(D, N) = (3031, 3599)
\]

Summary and Final Remarks

- The key to RSA security is the difficulty of factoring large composite numbers.
- Factoring \(N\) into its prime components is the critical first step in deriving the private key.
- Once \(p\) and \(q\) are known, calculating \(\phi(N)\) is straightforward.
- The modular inverse of \(E\) modulo \(\phi(N)\) gives the private exponent \(D\).
- In this example, we successfully deduced the private key \(D = 3031\) using basic number theory tools.

Additional Considerations

- The process outlined is theoretical and practical RSA implementations use much larger primes to ensure security.
- The security of RSA depends heavily on the difficulty of factoring large numbers; with small numbers like in this example, it is trivial.
- For real-world applications, primes are often hundreds or thousands of bits long, making factorization computationally infeasible with current technology.

Conclusion

Given the public key \((E=31, N=3599) \), we determined the private key exponent \(D = 3031\) by factoring \(N\), calculating \(\phi(N)\), and finding the modular inverse of \(E\). This process underscores the foundational mathematics of RSA cryptography and illustrates how the security of the system is rooted in number theory. Understanding these principles is crucial for both designing secure cryptographic systems and analyzing their security properties.

Frequently Asked Questions

How do you determine the private key in an RSA system when the public key is given as E=31 and N=3599?

To find the private key, you need to compute the private exponent D, which is the modular inverse of E modulo φ(N). First, factor N=3599 to find its prime factors, calculate φ(N), then find D such that (E D) ≡ 1 mod φ(N).

What are the initial steps to find the private key in RSA when E=31 and N=3599?

The initial steps involve factoring N=3599 into its prime factors, calculating φ(N) = (p-1)(q-1), and then computing the modular inverse of E=31 modulo φ(N).

How do you factor N=3599 to find the prime factors for the private key calculation?

You can factor 3599 by testing divisibility with prime numbers. For example, 3599 divided by 59 equals 61, so N=3599 factors into p=59 and q=61.

Once you have the prime factors p=59 and q=61, how do you compute φ(N)?

Calculate φ(N) = (p-1)(q-1) = (59-1)(61-1) = 5860=3480.

How do you find the private key D once φ(N) is known?

Find D such that (E D) ≡ 1 mod φ(N). Using E=31 and φ(N)=3480, compute D as the modular inverse of 31 modulo 3480, which can be found using the Extended Euclidean Algorithm.

What is the value of the private key D for E=31 and N=3599?

First, compute the modular inverse of 31 modulo 3480. Using the Extended Euclidean Algorithm, D = 2839. Therefore, the private key is D=2839.

Additional Resources

RSA Cryptography: Unveiling the Private Key from Public Parameters

In the realm of digital security, RSA (Rivest-Shamir-Adleman) stands as one of the most foundational and widely used cryptographic algorithms. Its strength lies in the mathematical complexity of factoring large composite numbers, which allows for secure key exchange and data encryption. When analyzing a specific RSA public key, such as E = 31 and N = 3599, a natural question arises: How does one determine the corresponding private key? This article delves into the intricate process

of deriving the private key, providing a comprehensive understanding of RSA's inner workings, from prime factorization to modular inverses.

Understanding RSA Public and Private Keys

The Core Components of RSA

RSA cryptography is based on a pair of keys:

- Public Key (E, N): Used for encrypting messages or verifying signatures.
- Private Key (D, N): Used for decrypting messages or signing data.

In our case, the public key is specified as:

- E = 31
- N = 3599

The goal is to find the private exponent D that pairs with the same modulus N, completing the private key.

The Mathematical Foundation

The security of RSA hinges on the difficulty of factoring the large composite number N into its prime factors p and q. Once p and q are known, the private key D can be computed using the Euler totient function φ(N):

$$
\phi(N) = (p - 1)(q - 1)
$$

The private exponent D is then the modular multiplicative inverse of E modulo φ(N):

$$
D \equiv E^{-1} \pmod{\phi(N)}
$$

Calculating D involves:

1. Factoring N to find p and q.
2. Computing φ(N).
3. Using the Extended Euclidean Algorithm to find D such that:

$$

```

of deriving the private key, providing a comprehensive understanding of RSA's inner workings, from prime factorization to modular inverses.

---

# Understanding RSA Public and Private Keys

## The Core Components of RSA

RSA cryptography is based on a pair of keys:

- Public Key (E, N): Used for encrypting messages or verifying signatures.
- Private Key (D, N): Used for decrypting messages or signing data.

In our case, the public key is specified as:

- E = 31
- N = 3599

The goal is to find the private exponent D that pairs with the same modulus N, completing the private key.

## The Mathematical Foundation

The security of RSA hinges on the difficulty of factoring the large composite number N into its prime factors p and q. Once p and q are known, the private key D can be computed using the Euler totient function φ(N):

$$
\phi(N) = (p - 1)(q - 1)
$$

The private exponent D is then the modular multiplicative inverse of E modulo φ(N):

$$
D \equiv E^{-1} \pmod{\phi(N)}
$$

Calculating D involves:

1. Factoring N to find p and q.
2. Computing φ(N).
3. Using the Extended Euclidean Algorithm to find D such that:

$$
```

$$
D \times E \equiv 1 \pmod{\phi(N)}
$$

Step-by-Step Derivation of the Private Key

Factoring N = 3599

The first essential step is to factor N into its prime factors p and q.

Method:

- Check for divisibility by small primes.
- Use trial division or more advanced factoring algorithms if needed.

Trial division process:

1. Test small primes:

- 2: 3599 is odd, so no.
- 3: Sum of digits = 3+5+9+9=26, not divisible by 3.
- 5: Last digit not 0 or 5.
- 7: 7×514 = 3598, close but not exact.
- 11: 11×327=3597, close but not exact.
- 13: 13×276=3588, no.
- 17: 17×211=3587, no.
- 19: 19×189=3591, no.
- 23: 23×156=3588, no.
- 29: 29×124=3596, no.
- 31: 31×116=3596, no.
- 37: 37×97=3589, no.
- 41: 41×87=3567, no.
- 43: 43×83=3589, no.
- 47: 47×76=3572, no.
- 53: 53×67=3551, no.
- 59: 59×61=3599 — Yes!

Result:

$$
p = 59,\quad q = 61
$$

Note: Since 59×61=3599, the factorization is confirmed.

Calculating Euler's Totient $\phi(N)$

$$
\phi(N) = (p - 1)(q - 1) = (59 - 1)(61 - 1) = 58 \times 60 = 3480
$$

Finding the Modular Inverse of E mod $\phi(N)$

We now need to find D such that:

$$
D \times E \equiv 1 \pmod{3480}
$$

which is:

$$
D \times 31 \equiv 1 \pmod{3480}
$$

This involves the Extended Euclidean Algorithm to compute the modular inverse.

Applying the Extended Euclidean Algorithm

Objective: Find integer D satisfying:

$$
31 \times D \equiv 1 \pmod{3480}
$$

Step-by-step process:

1. Compute $\gcd(31, 3480)$ using the Euclidean Algorithm.

- 3480 ÷ 31 = 112, remainder 8:

$$
3480 = 31 \times 112 + 8
$$

- 31 ÷ 8 = 3, remainder 7:

$$
31 = 8 \times 3 + 7
$$

- 8 ÷ 7 = 1, remainder 1:

$$
8 = 7 \times 1 + 1
$$

- 7 ÷ 1 = 7, remainder 0:

$$
7 = 1 \times 7 + 0
$$

Since gcd(31, 3480) = 1, D exists.

2. Work backwards to find D:

- From 8 = 3480 - 31×112
- From 7 = 31 - 8×3
- From 1 = 8 - 7×1

Substituting:

$$
1 = 8 - 7 \times 1
$$

but

$$
7 = 31 - 8 \times 3
$$

so

$$
1 = 8 - (31 - 8 \times 3) \times 1 = 8 - 31 \times 1 + 8 \times 3 = 8 \times 4 - 31
$$

Recall that

$$
8 = 3480 - 31 \times 112
$$

Substitute:

$$
```
```

$$
1 = (3480 - 31 \times 112) \times 4 - 31
$$

which simplifies to:

$$
1 = 3480 \times 4 - 31 \times 112 \times 4 - 31 = 3480 \times 4 - 31 \times (112 \times 4 + 1)
$$

Calculate:

$$
112 \times 4 = 448
$$

Thus,

$$
1 = 3480 \times 4 - 31 \times (448 + 1) = 3480 \times 4 - 31 \times 449
$$

Now, modulo 3480:

$$
D \equiv -449 \times 31 \equiv ? \pmod{3480}
$$

But more straightforwardly, D is congruent to the coefficient of 31 in the linear combination, which is -449. Since modular inverses are positive, we can add 3480:

$$
D = -449 + 3480 = 3031
$$

Therefore:

$$
D = 3031
$$

This D satisfies:

$$
31 \times 3031 \equiv 1 \pmod{3480}
$$

Final Private Key

Summary:

- Private exponent D = 3031
- Modulus N = 3599

Thus, the private key is:

$$
\boxed{
\textbf{D = 3031, N = 3599}
}
$$

Conclusion: Significance and Practical Implications

This detailed breakdown illustrates the core principles behind RSA key generation and recovery. By factoring the public modulus N into its prime factors p and q, calculating the totient, and then using the Extended Euclidean Algorithm, one can derive the private key exponent D. In real-world applications, RSA involves much larger prime numbers—often hundreds or thousands of bits long—to ensure security against factoring attacks. However, the fundamental mathematical process remains consistent.

Understanding this process not only demystifies RSA but also emphasizes the importance of choosing sufficiently large primes to prevent factorization. The example provided demonstrates that, given the public parameters, the private key can be systematically and precisely computed, highlighting both the elegance and the mathematical rigor of RSA cryptography.

In summary:

- The prime factors of N = 3599 are p=59 and q=61.
- The totient $\phi(N) = 3480$.
- The private exponent D, inverse of E=31 modulo $\phi(N)$, is 3031.
- The private key is (D=3031, N=3599).

This knowledge underpins the trustworthiness of RSA and demonstrates its reliance on fundamental principles of number theory and modular arithmetic.

In An Rsa System The Public Key Of A Given User Is E 31 N 3599 What Is The Private Key Of This

In An Rsa System The Public Key Of A Given User Is E 31 N 3599 What Is The Private Key Of This

Related Articles

- Help Quick Please! Which Deep-water Body Is A Unique Feature Of The Southern Ocean?The _____ Water
- In The Figure, The Light, Taut, Unstretchable Cord B Joins Block 1 And The Larger-mass Block 2 . Cord
- How Does The Author Of "History In The Making" Develop The Setting In The First Two Paragraphs Of The

Back to Home