Understanding Secure Internet Communication

por Mayko Silva

HTTP vs HTTPS: The Envelope Analogy

If you **seal the letter in an envelope**, only the recipient can open it. That's what **HTTPS** does—it encrypts your data so that even if someone intercepts it, they can't make sense of it.

Sealed Communication

HTTPS wraps your data in a secure envelope that can only be opened by the intended recipient.

Protection Layer

The encryption acts as a shield against potential eavesdroppers trying to access your sensitive information.

Secure Connection

The lock icon in your browser indicates that your connection to the website is encrypted and secure.

Two Ways to Encrypt Data

To keep information safe, we use **encryption**, which scrambles data so only the right person can read it. There are two main types:

Symmetric Encryption

Imagine you and a friend have a secret code. You use the same key to lock and unlock messages. It's **fast**, but the problem is: how do you safely share the key without someone else stealing it?

Asymmetric Encryption

This is like having **two keys**: one public and one private. You give your public key to anyone who wants to send you a secure message, but only **your private key** can unlock it. The good news? You don't need to worry about someone intercepting a secret key. The downside? It's **slower** than symmetric encryption.

The Best of Both Worlds

To keep things both **secure and efficient**, modern systems use **both methods** together. First, they use **asymmetric encryption** to safely exchange a **symmetric key**. Once that's done, they switch to **symmetric encryption** because it's much faster for data transfer.

Initial Handshake

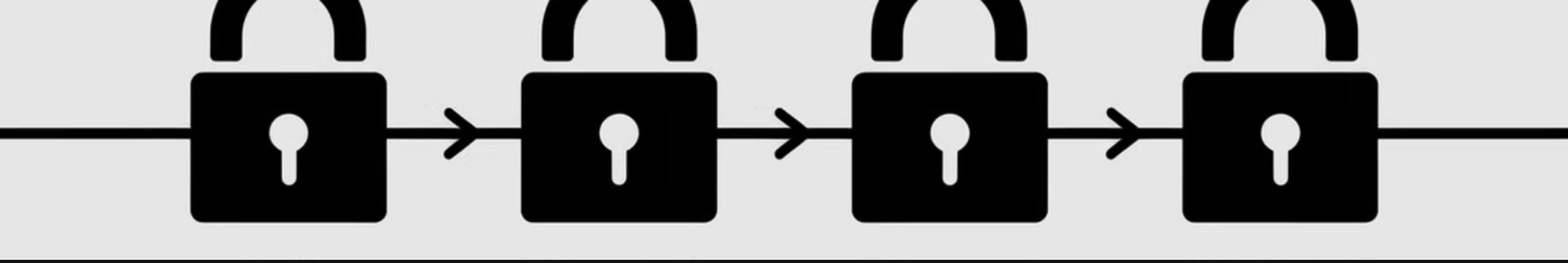
Systems establish contact using asymmetric encryption to verify identities securely.

Key Exchange

A symmetric key is securely shared using the asymmetric encryption channel.

Secure Communication

Once the symmetric key is exchanged, all further communication uses faster symmetric encryption.



SSL, TLS, and Secure Websites

Now, let's talk about **SSL and TLS**—the tech behind secure websites.

1 SSL Introduction (1994)

SSL (Secure Sockets Layer) was introduced by Netscape to encrypt web traffic. It went through several versions, but over time, vulnerabilities were found.

2 TLS Development

TLS (Transport Layer Security) replaced SSL as a **more secure** version and is now the standard for keeping web traffic safe.

3 HTTPS Implementation

HTTPS (the **S** stands for "Secure") uses **SSL/TLS** to encrypt your connection when you visit websites.

What About SAP Cloud?

If you're working with **SAP Cloud applications**, here's the good news: **SSL/TLS is required** and already **enabled by default in SAP BTP**. That means you don't need to manually activate anything—it's built-in to keep your data secure.

Default Security

SAP Business Technology Platform comes with SSL/TLS encryption enabled out of the box, ensuring your applications are secure from day one.

No Manual Setup

You don't need to configure encryption settings manually, saving time and reducing the risk of security misconfiguration.

Enterprise-Grade Protection

The built-in security meets enterprise standards, protecting sensitive business data across all SAP Cloud applications.

The Bottom Line

Secure communication is all about **encryption**—scrambling your data so only the right person can read it. Modern security uses a **mix of symmetric and asymmetric encryption** to balance **speed and safety**.

Encrypt

Data is scrambled using encryption algorithms

Transmit

Encrypted data travels securely across networks

Decrypt

Only authorized recipients can unscramble the data

Authenticate

Recipients verify they have the correct keys

Thanks to SSL/TLS, secure connections are standard across the web—including in SAP Cloud applications.

Key Takeaways

Understanding encryption is essential for secure internet communication. By combining different encryption methods, we achieve both security and performance in our digital interactions.

2

Encryption Types

Symmetric and asymmetric encryption work together to provide optimal security and performance.

1994

SSL Origin

The year Netscape introduced SSL, which eventually evolved into the more secure TLS protocol.

100%

SAP Cloud Security

All SAP Cloud applications have SSL/TLS enabled by default, ensuring complete protection.

With these security protocols in place, you can confidently send sensitive information over the internet, knowing it's protected from unauthorized access.