**HRM CODE TUTORIAL COLLECTION**

**Collection By:** R&D Team

Contents

[Content Security Policy 2](#_Toc62813334)

### A Deep Dive on End-to-End Encryption – How do Public Key Encryption Systems Work?

#### End-to-end encryption

End-to-end encryption đảm bảo rằng một message được chuyển thành một Secret Message bởi chính Original Sender (từ bản thân người gửi), và sẽ được decoded duy nhất bởi Final Recipient (người nhận cuối cùng của Message). Các cách Encryption khác sẽ được vào Encryption thực hiện bởi Third-parties. Điều đó nghĩa là những Parties đó phải được tin tưởng với Original Text. End-to-end Encryption về tổng thể sẽ an toàn hơn, bởi vì chúng giảm đi số lượng các Parties có thể tham gia vào quá trình break Encryption.

Nếu sử dụng một cách chính xác end-to-end encryption có thể hỗ trợ việc bảo vệ nội dung các Messages, Text, hoặc thậm chí là Files để tránh việc một ai đó có thể đọc được ngoại trừ người nhận cuối. Nó cũng có thể được sử dụng để hỗ trợ việc đảm bảo Message được gửi tới một ai đó sẽ không bị chỉnh sửa.

Trong những năm gần đây, end-to-end encryption Tools đã có thể được sử dụng rộng rãi. Secure Messaging Tools như Signal (iOS, Android) cho Voice calls, Video calls, Chats và File sharing là một ví dụ về ứng dụng sử dụng end-to-end encryption để mã hóa Message giữa người gửi và người nhận. Những Tools này làm cho các Message trở thành Unreadable đối với Eavesdroppers (người nghe lén) trên Network, và đối với cả bản thân Service Provider.

Và bởi vì những lý do trên, cách triển khải của end-to-end encryption có thể khá khỏ để hiểu và sử dụng đúng cách. Và trước khi chúng ta muốn sử dụng một end-to-end encryption Tools, trước tiên chúng ta có thể tìm hiểu qua căn bản của một Public Key Cryptography

Public Key Encryption

Các Traditional Encryption Systems sử dụng cùng một Secret, hoặc Key để encrypt và decrypt một Message. Bởi vậy nếu encrypt một File với Password là “somewhatss”, chúng ta sẽ cần cả File và Password “somewhatss” để decode.

Public Key Encyption, hoặc Public Key Cryptography, là một phương thức mã hóa dữ liệu sử dụng hai Keys khác nhau, và một trong hai Keys, Public Key có thể được sử dụng bởi bất kỳ ai. Key còn lại được gọi là Private Key. Dữ liệu được mã hóa bởi Public Key chỉ có thể được giải mã bởi Private key, và dữ liệu được mã hóa bởi Secret Key chỉ có thể được giải mã bởi Public Key. Public Key Encryption còn được biết tới với tên Assymetric Encryption (mã hóa bất đối xứng). Và nó được sử dụng rộng rãi cho TLS/SSL, thứ mà làm nên HTTPS

#### What does Encyption Do?

Cách mà Encryption hoạt động khi gửi một Secret Message

1. Một Readable Message (“heello ???”) được mã hóa thành một Encrypted Message không thể hiểu bởi bất kỳ ai khi đọc nó (“FDSbnnn41NNN+ooonnnhh”)
2. Encrypted Message sau đó sẽ được gửi đi qua Internet (nếu ai đó đọc được Message này thì nội dung chỉ là “FDSbnnn41NNN+ooonnnhh”
3. Khi Encrypted Message được gửi tới đích (người nhận cuối), và chỉ duy nhất người dùng cuối này, bằng một cách nào đó có thể giải mã được Encrypted Message thành Original Message (“heello ???”)