JavaScript による End-to-End セキュリティ

公開鍵暗号はどうやって使えばいいのか？ 編

栗原 淳

September 3, 2019

はじめに

はじめに

前回・前々回 (第 1,2 回) では

- End-to-End (E2E) セキュリティの原則と必要性
- Web サイトでの E2E セキュリティ実践のため、JavaScript での暗号 (AES) の正しく・安全に利用するする方法

を勉強した。

ところで、AES(共通鍵暗号) とは別に、「公開鍵暗号」というのが存在する。

今回は正しく・安全に公開鍵暗号を使ってみる方法、についてのお話。

この講義で最終的に学びたいこと

- 公開鍵暗号ってどういうもの？AES とのメリデメは？
- RSA と楕円曲線の違い。
- AES と公開鍵暗号を組み合わせてデータを暗号化するために。

細かい所の話もしますが、なるべく数式とか使わないで「イメージ」でわかるようにしていきます。

この講義の対象と事前準備

対象:

- 暗号・セキュリティ技術に興味がある初学者
- Web に暗号技術を導入したい Web 系のエンジニア

必須ではないが触って楽しむのには必要な事前準備:

- Git が使えるようになっていること
- Node.js が使えるようになっていること
- Google Chrome 系ブラウザ and/or Firefox が利用可能なこと

公開鍵暗号の使い方 事始め

まとめ

まとめ

お疲れ様でした。

- 公開鍵暗号を利用する際のお作法を学んだ。

次回以降…リクエスト次第ですが、

- 「情報が改ざんされてない」ことを保証するために（電子署名と MAC）
- RFC とアルゴリズム・フォーマット

などを予定。

宣伝 1

E2E 暗号化ファイル転送サービス「iTransfy」を提供しています。

宣伝 2

Zettant ではイケイケの仲間を募集しています。

1. 今回は共通鍵暗号
2. 公開鍵暗号& Hybrid Encryption
3. ハッシュ・署名と HMAC
4. 超マニアック講座：RFC とアルゴリズム・フォーマット

Appendix

This page is not counted.