インターネットの安全性を検証する

Verify Internet Security

木村 大樹 Taiki Kimura
瀬尾 孝幸 Takayuki Seo
舟橋 知論 Tomonori Funahashi
塚田 将太 Shota Tsukada
横関 秀樹 Hideki Yokozeki
平山 力地 Rikichi Hirayama
菊池 勇幸 Yuko Kikuchi
辻 貴文 Takahumi Tsuji
松橋 みどり Midori Matsuhashi
小林 峻 Shun Kobayashi
中里 翔太 Shota Nakasato
永谷 弘宣 Hironobu Nagaya

概要 Outline

本プロジェクトでは、公開鍵暗号方式の 1 つである RSA 暗号を実装し、それに対する解読法とその対策について扱う。具体的には、RSA 暗号に対するタイミング攻撃を行う。タイミング攻撃とは暗号化・復号化にかかる時間を利用する攻撃法のことであり、この攻撃法により約 2 時間で解読されたという報告がある (2003, Boneh, Brumley)。本プロジェクトの課題としては、RSA 暗号を実装し、それに対する攻撃を行う。さらに、それらの攻撃に対する対策をする。

In this project, we implement the RSA cryptosystem that is the one of the public key cryptosystem. Then we Timing attack it, and take counter measures. Timing attack is cracking using the time that coding / decoding takes, and there is a report cracked in about 2 hours by this attack. In the task of this project, we implement an RSA cryptosystem and perform attack for it. Furthermore, we do counter measures for those attack.

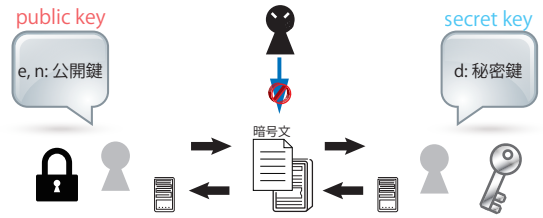
RSA 暗号 RSA Cryptosystem

RSA 暗号は、1977 年に Rivest、Sharmir、Adleman の 3 人によって発表された最初の公開鍵暗号方式である。この RSA 暗号は、公開鍵暗号としてもっとも多く利用されている。

以下に、公開鍵暗号方式と本プロジェクトで利用するタイミング攻撃について概要を示す。

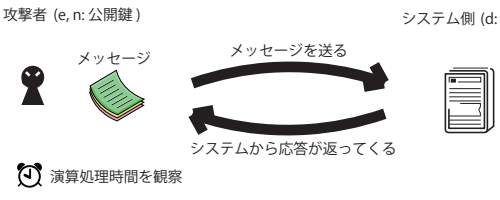
RSA Cryptosystem is invented by Rivest, Sharmir, and Adleman. It is widely used all of the world.
We show about RSA Cryptosystem and Timing Attack bellow.

RSA 暗号方式 RSA Cryptosystem



公開鍵と秘密鍵が異なっているのが特徴

タイミング攻撃 Timing Attack



メッセージに対する演算処理時間を繰り返し観察することで秘密鍵 (指数 d) を推定することが可能

暗号技術によって

第３者の盗聴、なりすまし、改ざんなどから情報を守る！

なぜ鍵の推定が可能か？

法を n より小さい数字にすると計算時間が短くなる。逆に大きい数字にすると計算に時間がかかる。その差を徐々に狭めていくと n に近づいていくため推定が可能である。

後期課題 Task (later term)

RSA 暗号の高速化、及びそれに対する攻撃と防御

We accelerate the speed of RSA proccessing. And then, we timing attack on the scheme and take counter measures.

Group A

高速化班

RSA 暗号の高速化と攻撃に対する防御

Accelerating the speed of RSA proccessing and taking counter measures in case of Timing attack.

Group B

攻撃班

RSA 暗号に対する攻撃の実装

Timing attack on RSA cryptosystem