暗号技術入門

第5章「公開鍵暗号」①

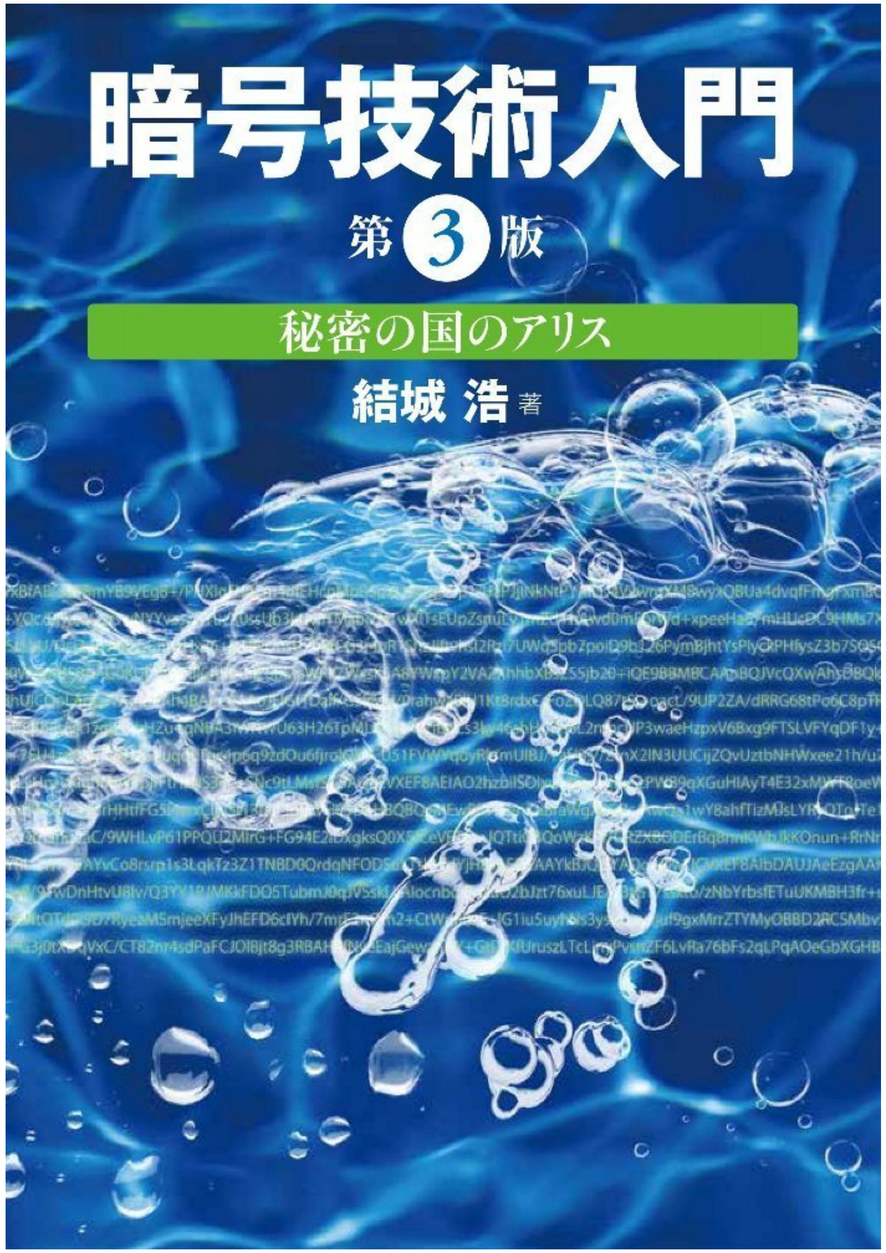
鍵配送問題と公開鍵暗号

暗号技術入門

出版：SB Creative

著者：結城 浩

第三版は2015年発行。暗号化技術の基礎から丁寧に解説されており、各所で初心者にお勧めされている。改訂版ではビットコインなど最新の情報も記載。



公開鍵暗号

公開鍵暗号

・コインロッカーの例えが秀逸。

・ロッカーに荷物を入れる、コインを投入してキーを抜き取る。
　これでロッカーを閉じることができる。キーがなければロッカーは開かない。

・コインがあれば誰でも閉じることができる。
　けれど一旦閉じるといくらコインを投入しても鍵は開かない。

・ロッカーを開けるには閉じた時に抜き取ったキーが必要。

・コインはロッカーを**閉じるための鍵**、キーはロッカーを**開けるための鍵**と言える。

鍵配送問題

鍵配送問題

- 対象暗号では複合化するために、暗号化した際に用いた鍵が必要。
- 盗聴の可能性があるから暗号化するので、当然暗号文と同様の手段では鍵配送はできない。
- 通信路を暗号化するのも手。その暗号アルゴリズムが知られない限りは安全。
  しかし「隠すことによるセキュリティ」は危険。

鍵配送問題の解決

・以下の方法が用いられる。

・鍵の事前配布

・鍵配布センターの利用

・Diffie-Hellman鍵交換

・公開鍵暗号

鍵の事前配布による解決

- 最も簡単な解決方法。
- **安全な方法で事前に**鍵を渡しておく。

- ただし、これには限界がある。
- そもそも事前に安全に渡す策がない場合もある。
- 事前共有ができたとしても、対象が大人数になると現実的でない。
- 例えば1,000人の会社で、自分以外の999人と通信する可能性があるとすると、鍵は49万9500個必要になる。流石に無理。

鍵配布センターの利用による解決

- 中央に鍵管理センターを設置しセンターで鍵を作成する。
  各人はセンターとの鍵の事前共有だけで済む。
- センターには全員の鍵があり、データベースで管理する。

- 通信時の手順は次

鍵配布センターの利用による解決

アリスがボブに暗号メールを送りたいとする。

(1) アリスがセンターに対しボブとの通信を申請。

(2) センターは擬似乱数生成機を使いセッション鍵を生成。

(3) センターは両人の鍵をデータベースから取得。

(4) センターはアリスの鍵を使いセッション鍵を暗号化、アリスへ送付。

(5) センターはボブの鍵を使いセッション鍵を暗号化、ボブへ送付。

(6) アリスはセッション鍵を復号化する。

(7) アリスはセッション鍵を使いボブへの暗号メールを作成し送付。

(8) ボブはセッション鍵を復号化する。

(9) ボブはセッション鍵を使ってアリスからのメールを復号化する。

(10) アリスとボブはセッション鍵を廃棄する。

鍵配布センターの利用による解決

やってられん

センターが攻撃されるとおしまい

Diffie-Hellman鍵交換による解決

・送信者と受信者が情報を相互に受け渡しをする。

アリスとボブの例で考える。

・アリスとボブが互いにある情報を交換する。この情報は盗聴されても構わない。

・両者は交換した情報を元に、同じ鍵を生成できる。しかし盗聴者には不可能。

…?

詳しくは第11章で。

公開鍵暗号による解決

- 「暗号化の鍵」と「復号化の鍵」が同じである対象暗号とは違い、
  ふたつの鍵は全く別のものを使う。
- 「暗号化の鍵」を持っている人なら誰でも暗号化が可能。
- しかし復号できるのは「復号化の鍵」を持っている人のみ。

- 受信者は前もって暗号化の鍵を送信者に知らせておく。
  これはいくら盗聴されても問題はない。
- 送信者は受け取った鍵で暗号化し送信する。
- 受信者は自身が持っている復号化の鍵で復号する。

公開鍵暗号

公開鍵暗号

- 「暗号化の鍵」＝「**公開鍵 (public key)**」
- 「復号化の鍵」＝「**秘密鍵 (private key)**」
- 2本は対になっている。ので**鍵ペア**と呼ぶ。
- 2本には数学的な密接な関係が存在する。別個に作ることは不可能。

- 公開鍵はいくら外部に漏れようと関係ない。
- が、秘密鍵は絶対に公開してはならない。

公開鍵暗号の歴史

- 1976年、DiffieとHellmanが公開鍵暗号のアイデアを公開。アルゴリズムは非公開。
- 1977年、MerkleとHellmanがアルゴリズムとしてナップザック暗号を作成。
  特許取得するも安全でないことが明らかに。
- 1978年、**R**on, **S**hamir, **A**dlemanが公開鍵暗号アルゴリズム、RSAを発表。
  いわゆるRSA暗号。現代のデファクトスタンダードとなった。

公開鍵暗号の課題

・公開鍵暗号でも解決できない課題がある。

・入手した公開鍵が、本当に正しい公開鍵なのかを判断する必要がある。

・**鍵検証**の問題

・後ほど解説。

・また、対象暗号と比べて何百倍も遅いという問題もある。

・この問題の解決方法については第6章で。