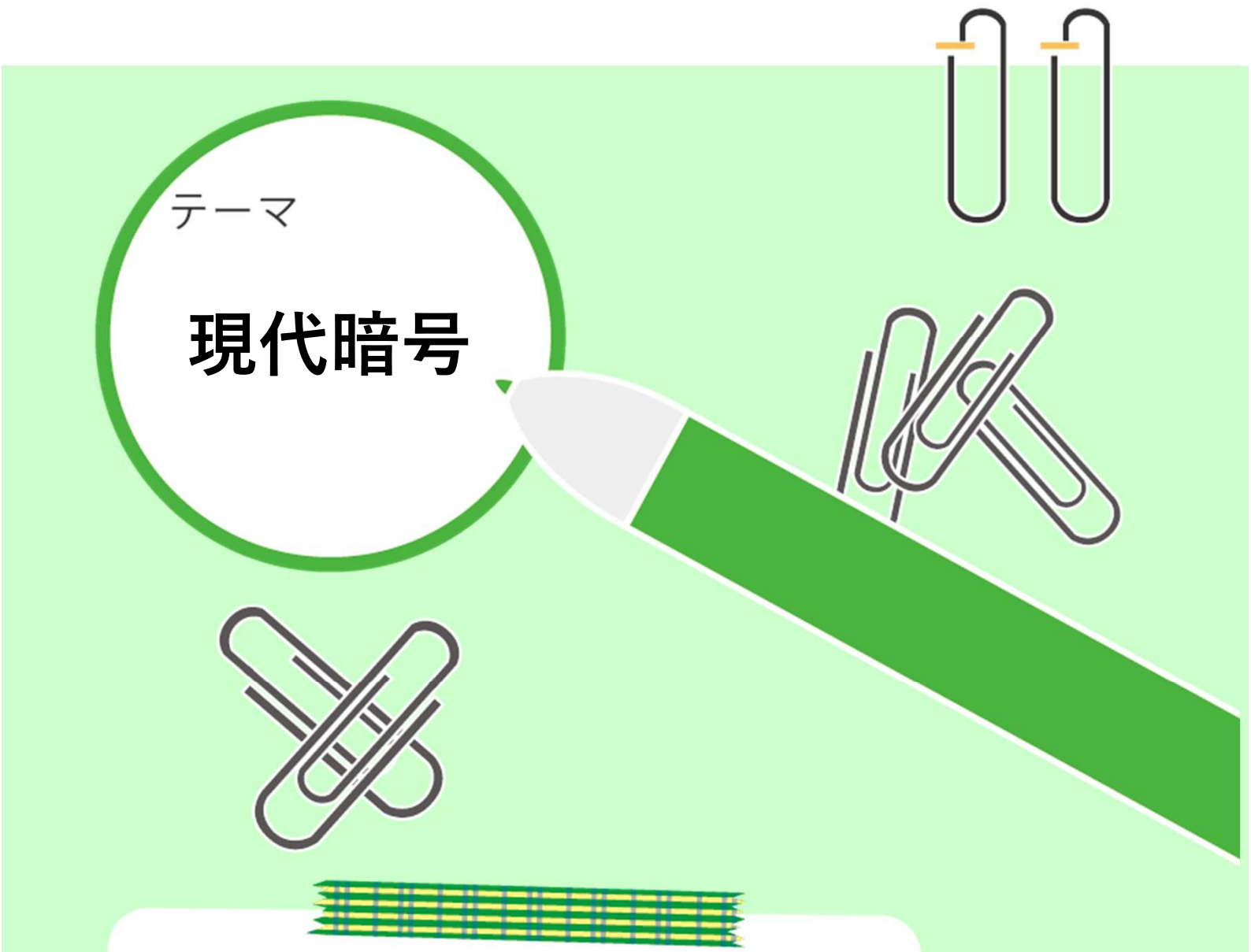
さくっと



テーマ

現代暗号

「さくっと」とは？
興味のある分野について、さくさくと勉強が進むように作成された調べ方ガイド（パスファインダー）です。
みなさんの学習支援を行う図書館学生サポーターが作成しました。
ぜひ学習の際に参考にしてください。

図書館学生サポーター　茂木

1.はじめに

一般に暗号と呼ばれるものはクイズやフィクションに代表されるように, 秘密のアルゴリズム, もしくは図や表を用いて,情報の受け渡しを行うことを目的とするものである. これを古典暗号という.

現代暗号とは

一方,現代暗号は, 数学的に解くことが難しい問題を安全性の根拠とすることで, 仮に暗号化アルゴリズムが既知であったとしても, 通信や計算機上の情報の保護を可能とする暗号方式を指す.
日常生活において, 暗号化の方式やその安全性について意識することは少ない.
しかし, 現代暗号について学ぶことで, 計算機の進化や情報通信技術の変遷, 数学と情報の関連を知ることができる.
何より, 攻撃者の存在を前提とした学問は無二であるため, この記事を読み現代暗号に興味を持たれたのであれば3.に示すような参考文献を通じて興味を深めていただきたい.

発展分野

量子コンピュータ を用いることで, 既存の暗号方式が安全性の根拠としている問題を, 現実的な時間で解くことができると考えられている. そこで, 量子コンピュータでも破れない暗号である耐量子計算機暗号に興味のある方に向けて, 入門書を参考文献に示す.

関連キーワード
暗号理論, セキュリティ, 耐量子暗号, 公開鍵暗号, 共通鍵暗号, 秘密計算

2.学ぶためのポイント

理論を学ぶのであれば代数学, 整数論, 情報理論等の知識が必要となるが, 専門書の1章で解説されることも多いため, 適宜参考書を確認すればよい.

実装の部分を学ぶのであれば, プログラミングやアルゴリズム, 論理回路の知識があることが望ましいが必須ではない.

3.学習のために

- 一般向けに書かれた本

暗号解読 : ロゼッタストーンから量子暗号まで. サイモン・シン,青木薫訳
飯塚分館閲覧 3 階語学, 809.7||S-1, 006036069

3.学習のために 続

● 学び初めにおすすめの本

・代数学から学ぶ暗号理論-整数論の基礎から楕円曲線暗号の実装まで. 宮地充子
飯塚分館閲覧３階工学・技術, 548.91||M-13, 006079253

・暗号理論入門. 岡本栄司
飯塚分館閲覧３階工学・技術, 549.9||O-138,6012049

● 学びを深めるために(耐量子計算機暗号)

・耐量子計算機暗号. 縫田光司
飯塚分館閲覧３階Staff Picks, 548.91||N-38, 006083756

・格子暗号解読のための数学的基礎:格子基底簡約アルゴリズム入門. 青野良範, 安田雅哉
戸畑本館閲覧室３階, 410||A-20, 001110909

現代暗号に関する動向

NTT社会情報研究所の技術ジャーナル
https://www.rd.ntt/research/index.html?lab=15
米国立標準技術研究所
https://www.nist.gov/news-events/news-updates/topic/248746

関連する研究室

九州工業大学　荒木研究室
筑波大学　暗号理論研究室
東京大学 高木・高安　暗号数理情報学研究室

4.参考文献

九州工業大学情報セキュリティ講義資料