あなたの身の回りの暗号は大丈夫？

計算量理論と暗号の安全性

NII

どんな研究？

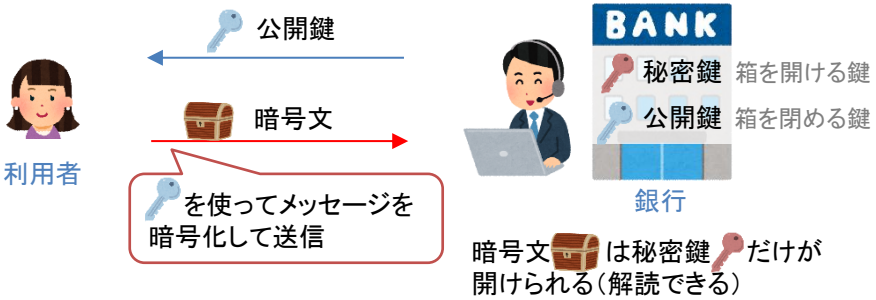
日常生活において、クレジットカードの番号を入力したり、銀行にパスワード送る場合、途中で盗聴されても解読できないように暗号化の技術が用いられいます。しかし、現在広く使われている暗号は本当に安全かどうかわかっていません。暗号の安全性は、ある計算問題の難しさに基づいています。計算量理論とはそのような計算の困難性を追求する学問です。

何がわかる？

- 暗号化技術とは？
- なぜ安全性がわかっていないのか
- P ≠ NP 予想（１００万ドルの懸賞問題）
- 計算量理論の最先端の研究

暗号と P ≠ NP予想

公開鍵暗号方式：事前に鍵を共有しなくても安全に通信できる方式



暗号文は秘密鍵だけが開けられる（解読できる）

P ≠ NP予想：懸賞金１００万ドル！ミレニアム懸賞問題

正しさを簡単に検証できるが、答えを見つけるのが計算困難な問題が存在するか？

↦

例：素因数分解は掛け算と同じくらい素早く計算できるか？

もしP = NPならば、安全な公開鍵暗号方式は存在しない！　最先端の研究：逆は成立するか？

P ≠ NP予想

P = { 効率的に計算できる問題全体 }　例：掛け算 ∈ P

NP = { 効率的に解の正しさを検証できる問題全体 }

例：素因数分解 ∈ NP，掛け算 ∈ NP

入力 863 × 941 解（素因数）（素因数）

掛け算 →

← 素因数分解

解 812083 入力

（計算にはとても長い時間がかかると予想されている）