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？

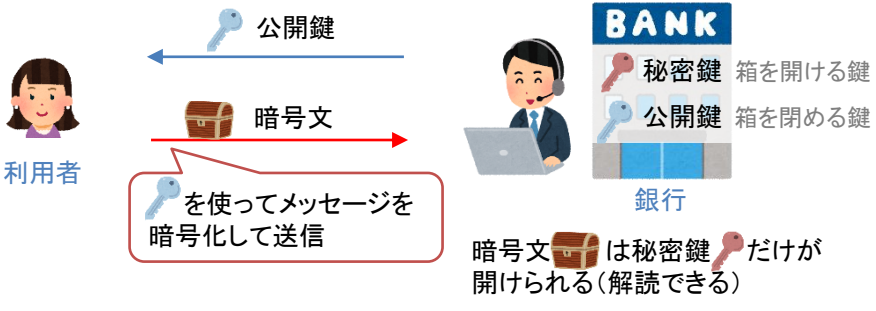
日常生活において、クレジットカードの番号を入力したり、銀行にパスワード送る場合、途中で盗聴されても解読できないように暗号化の技術が用いられいます。しかし、現在広く使われている暗号は本当に安全かどうかわかっていません。暗号の安全性は、ある計算問題の難しさに基づいています。計算量理論とはそのような計算の困難性を追求する学問です。

## 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）
- 五つの可能世界
- どのようなアプローチで進展を目指しているか

## 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




**P ≠ NP予想**：懸賞金１００万ドル！ミレニアム懸賞問題

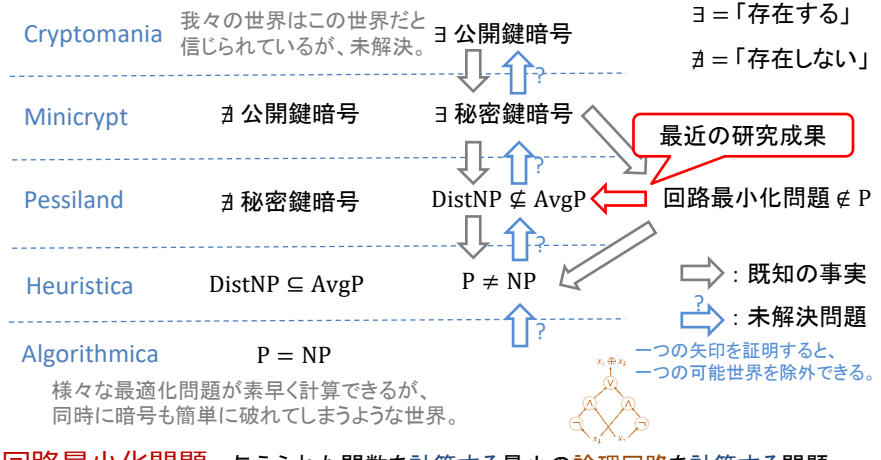
正しさを簡単に検証できるが、答えを見つけるのが計算困難な問題が存在するか？

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！

## 五可能世界と回路最小化問題

- 計算量理論の知識と一貫性がある五つのありうる世界がある。
- その中で、ちょうど一つだけが我々の真の世界に対応する。




回路最小化問題　与えられた関数を計算する最小の論理回路を計算する問題