暗号を知ろう!!

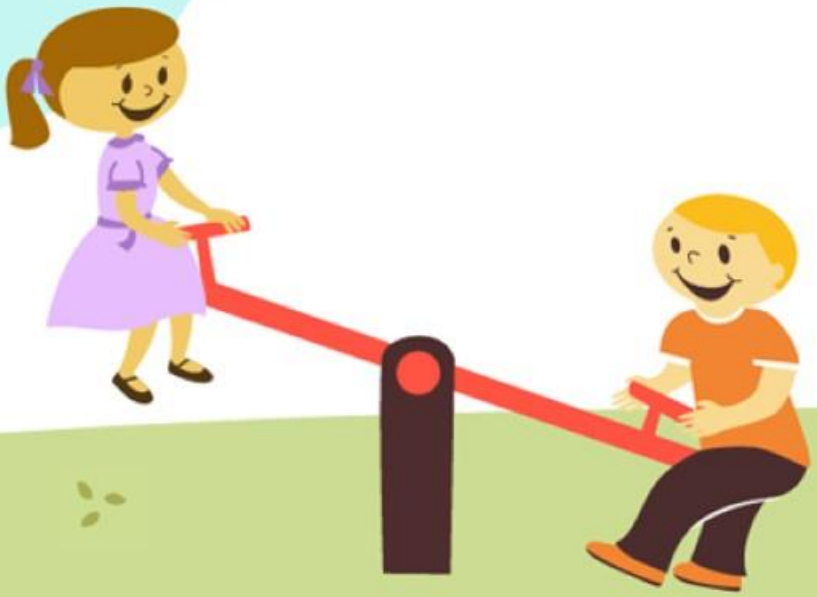
セキュリティーの代名詞的存在を理解する

2023年6月-日

本日の内容

1. そもそも暗号って何？なんで使うん？
2. 暗号小史
3. コンピュータの暗号　＆　実際に触れてみる

そもそも**暗号**って何？
なんで使うん？



暗号って何？

なんらかの手法を用いて、文章や信号などの**情報を難読化**し、特定の対象者のみが情報を享受できるようにしたもの。

情報を制する者は戦いを制す

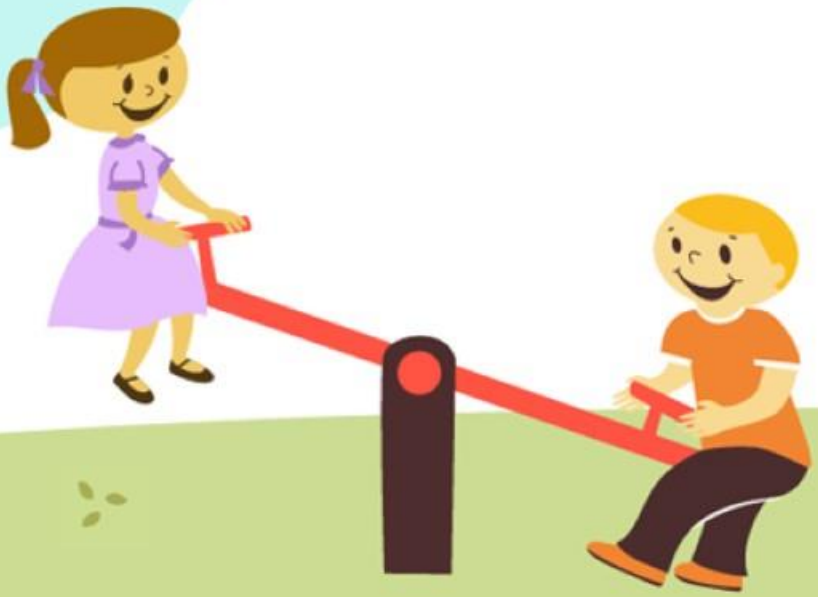
つまり**暗号を完全に理解**すれば最強？！

用語

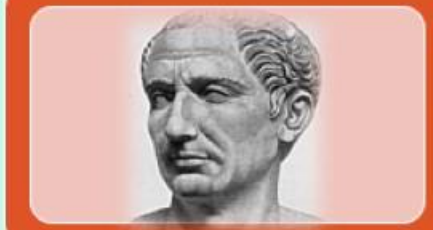
- 平文：暗号化する前の文章やデータ。そのままでは危険！
- 暗号化：平文を暗号化すること
- 復号化：暗号文を平文にすること
- 鍵：平文を暗号化したり、複合化するために必要。アルゴリズムによって異なる。

暗号小史

昔から利用されている



時代とともに進化してきた暗号



紀元前５００～１００年頃

- シーザー暗号
- スタキュレー暗号

２０世紀前半（世界大戦期）

- 紫暗号
- エニグマ暗号

２０世紀後半～（コンピュータの時代）

- RSA暗号
- 量子暗号

ざっくり暗号

▪ シーザー暗号

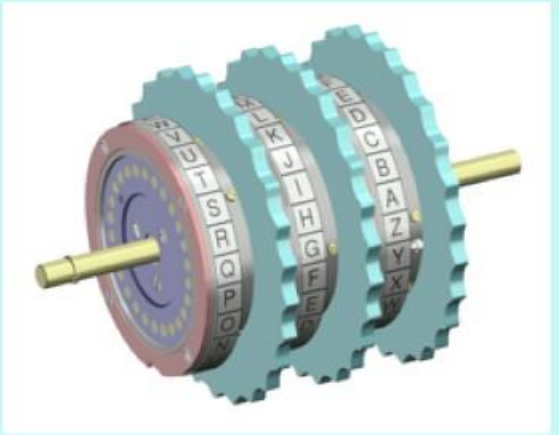
単換字式暗号

通常のアルファベット:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

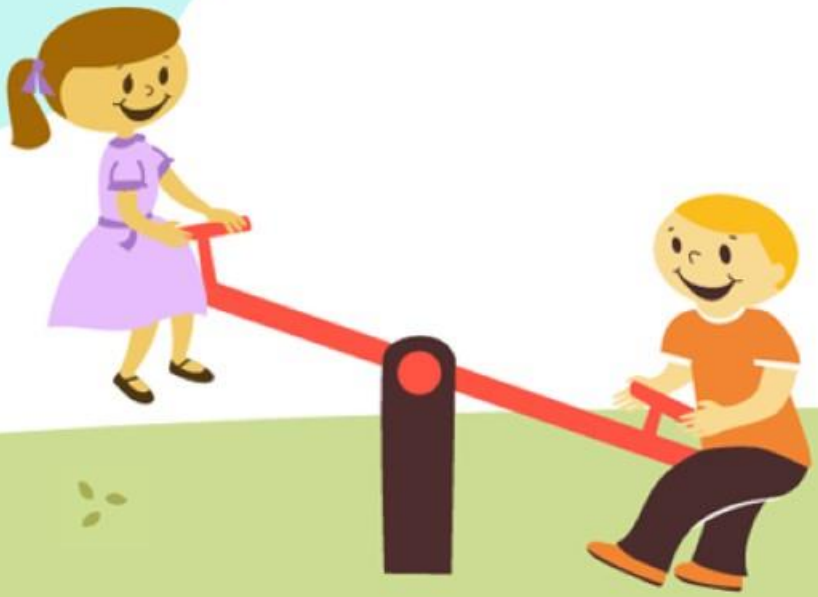
暗号化アルファベット:
XYZABCDEFGHIJKLMNOPQRSTUVW

▪ パープル, エニグマ暗号

機械式暗号



ローター



コンピュータの暗号

暗号は身近なものに利用されています

主に2種類に大別される

・共通鍵暗号方式

- 暗号化と複合化を同じ鍵で行う。
- 暗号する側と複合する側で全く同じ鍵を持つ必要がある。

・DES暗号
・AES暗号

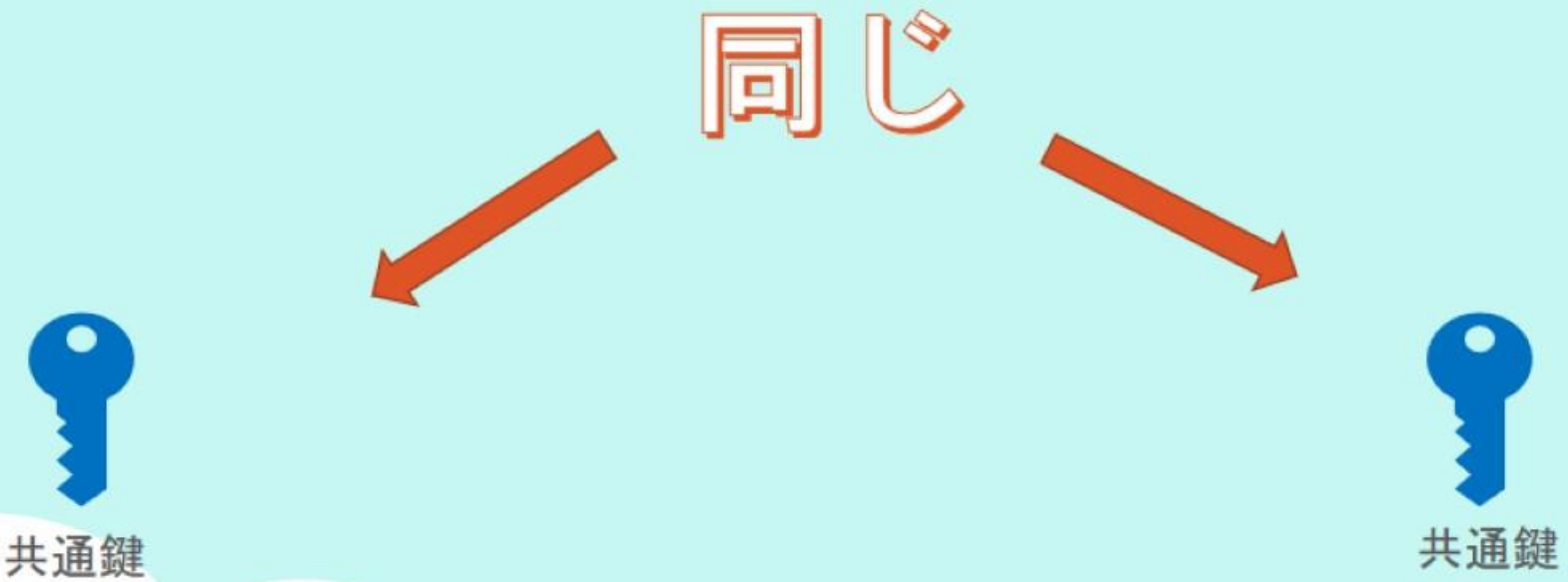
・公開鍵暗号方式

- 暗号のための**秘密鍵**と復号や署名検証に用いられる**公開鍵**がある。

・RSA暗号

・共通鍵暗号方式

・共通鍵暗号方式



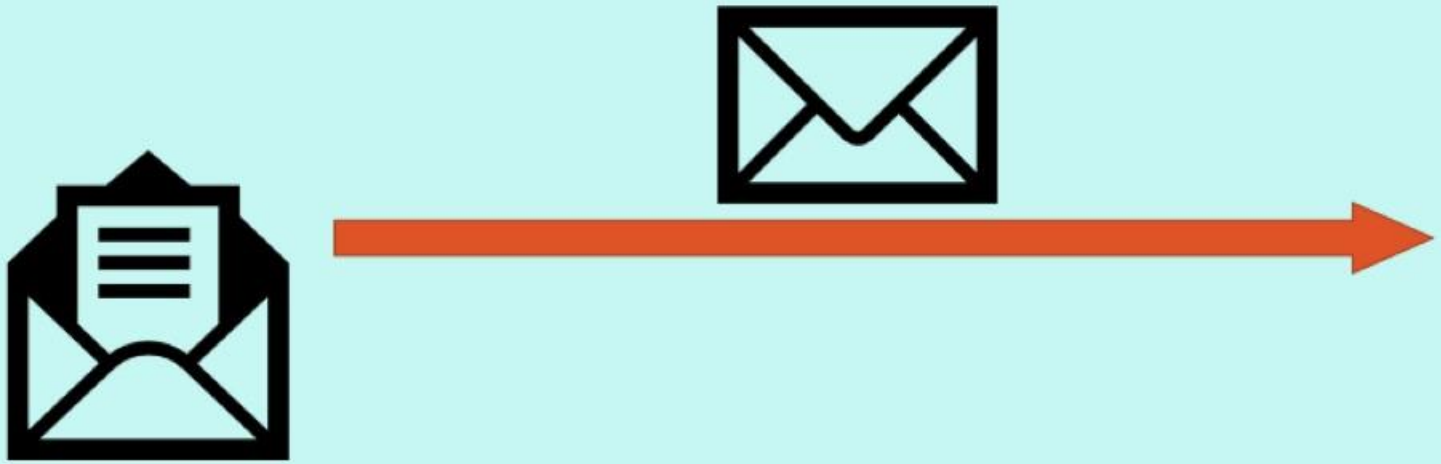
・共通鍵暗号方式

暗号化

共通鍵

共通鍵

・共通鍵暗号方式

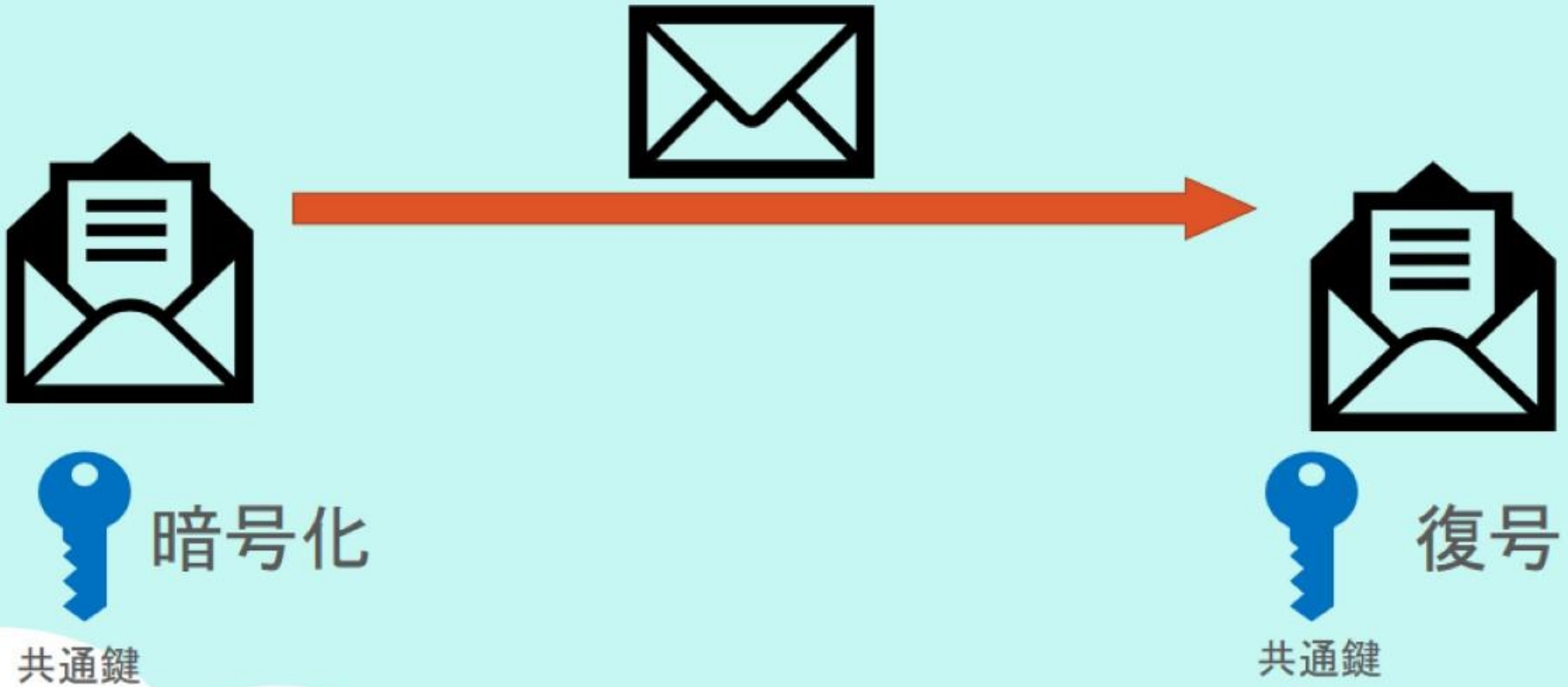


暗号化

共通鍵

共通鍵

・共通鍵暗号方式



・共通鍵暗号方式

共通の鍵を事前に送る必要がある。

鍵が盗聴されてる
危険がある

暗号化

共通鍵

復号

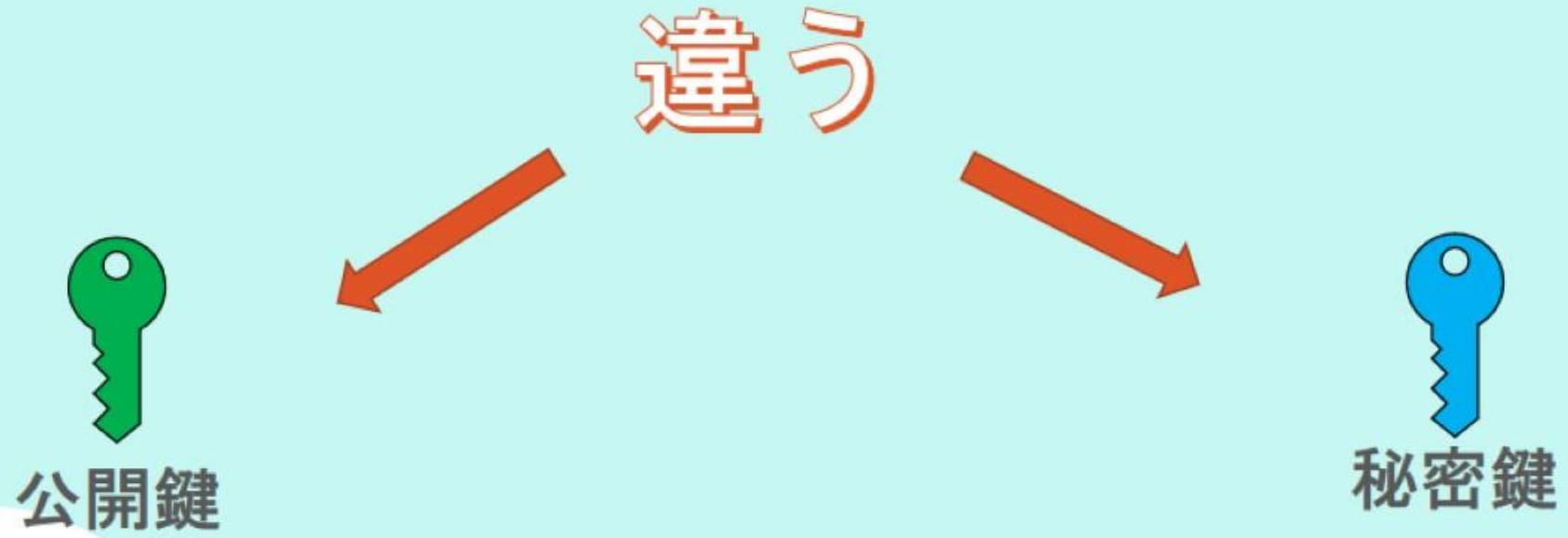
共通鍵

・公開鍵暗号方式

公開鍵

秘密鍵

・公開鍵暗号方式

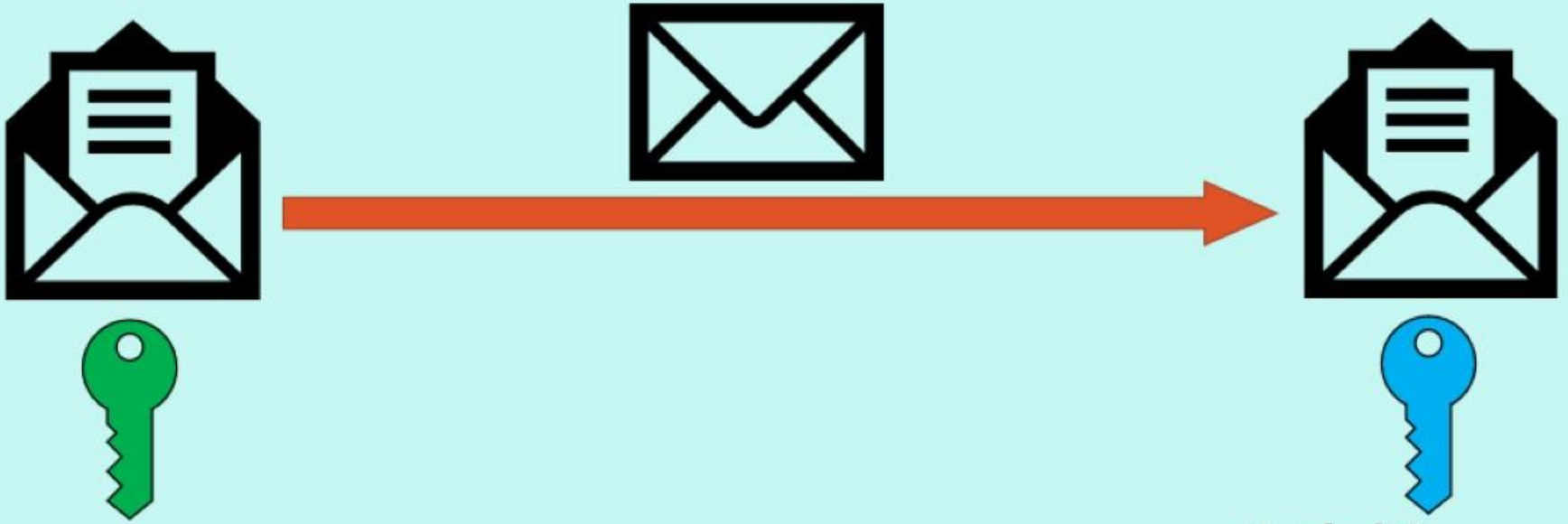


・公開鍵暗号方式

公開鍵で暗号化

秘密鍵

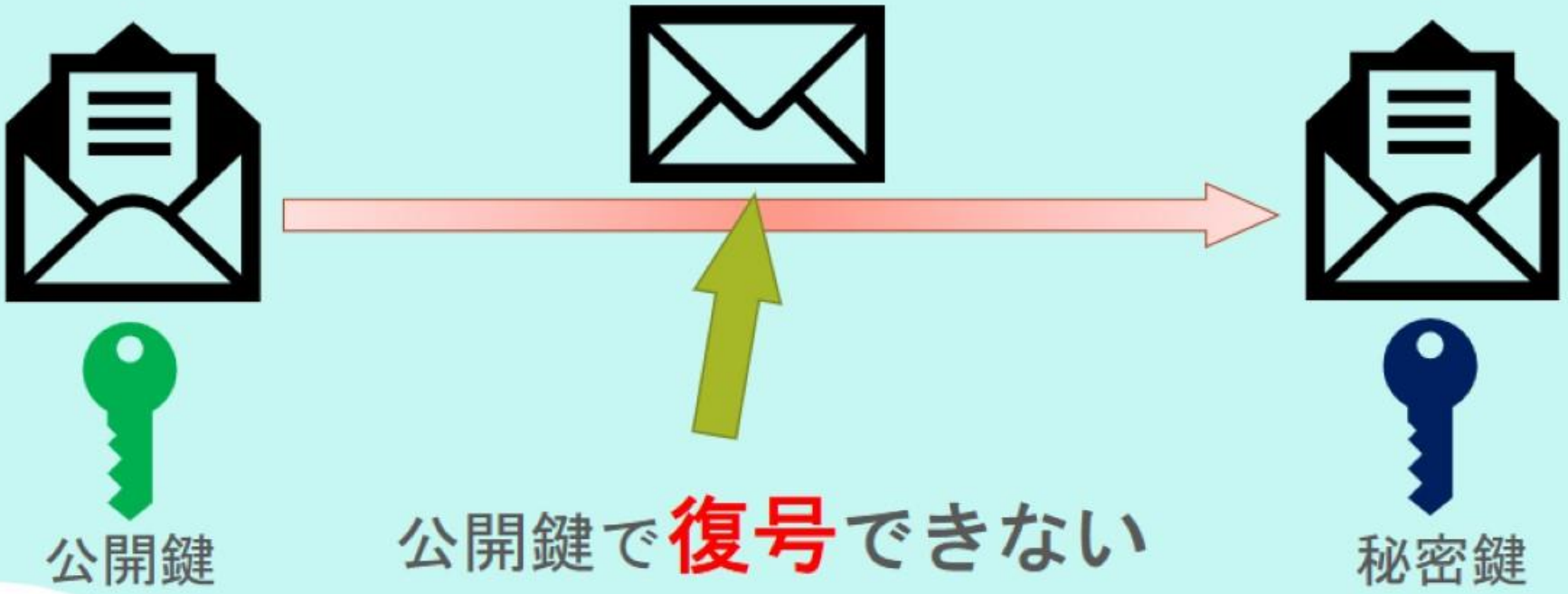
・公開鍵暗号方式



公開鍵で暗号化

秘密鍵で復号

・公開鍵暗号方式



・実用例

https通信で用いられている

・実用例

利用者

共通鍵

サーバー

公開鍵

秘密鍵

証明書

・実用例

利用者

共通鍵

接続要求

サーバー

公開鍵　秘密鍵

証明書

・実用例

・実用例

利用者

サーバー

秘密鍵

公開鍵

公開鍵で暗号化された
共通鍵

・実用例

利用者

サーバー

秘密鍵

・実用例

利用者

サーバー

秘密鍵

秘密鍵で復号化

・実用例

利用者

サーバー

秘密鍵

秘密鍵で復号化

・実用例

利用者

サーバー

webページ

共通鍵で復号

共通鍵で暗号化

・ハッシュ関数

任意の長さのデータを、一定の長さのデータに変換する
"**関数（アルゴリズム）**"

・デジタル署名

秘密鍵

公開鍵

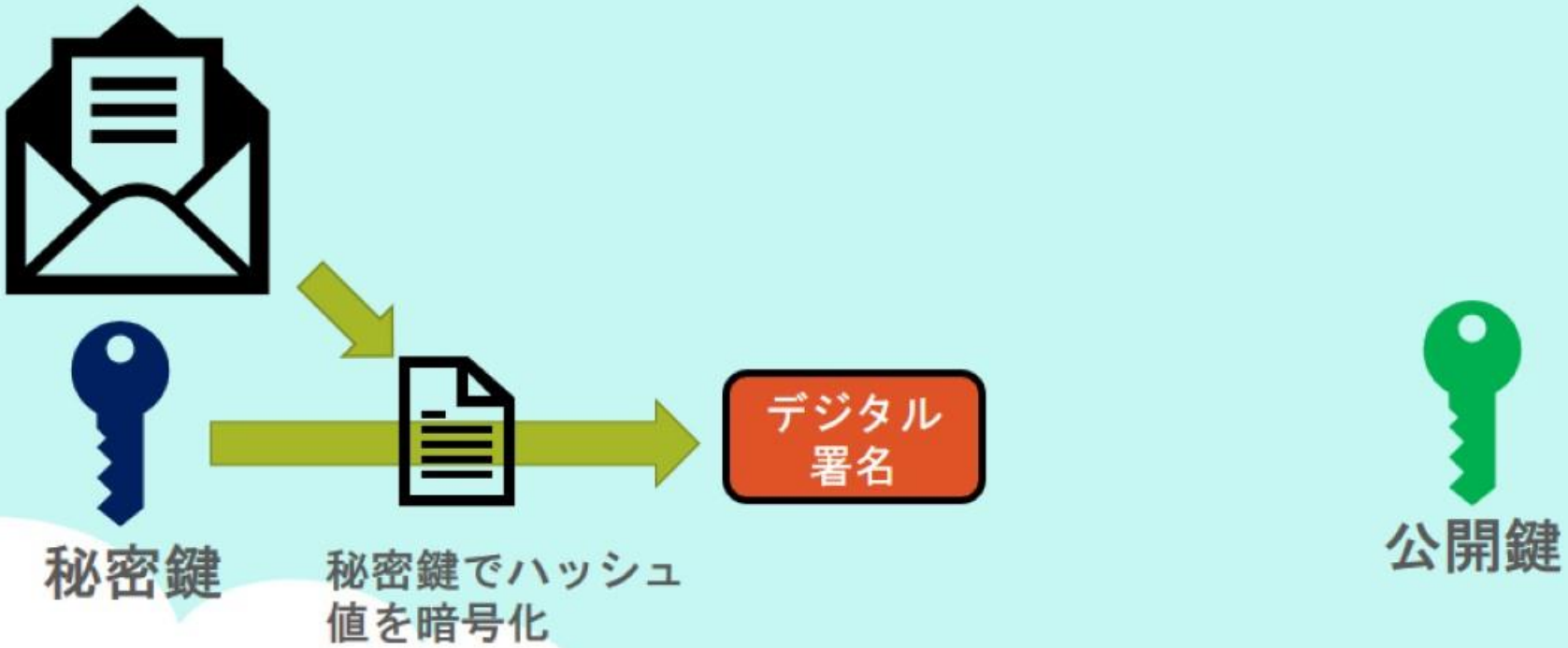
・デジタル署名

秘密鍵

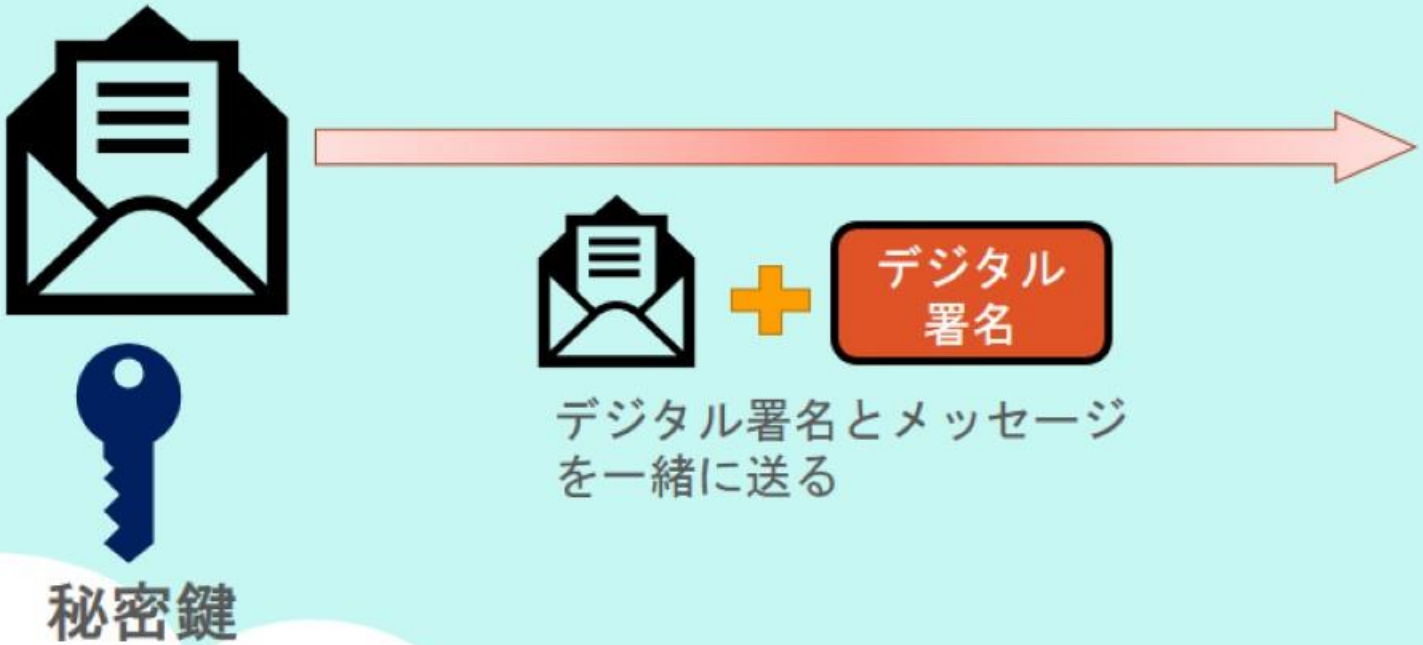
メッセージから
ハッシュ値を作る

公開鍵

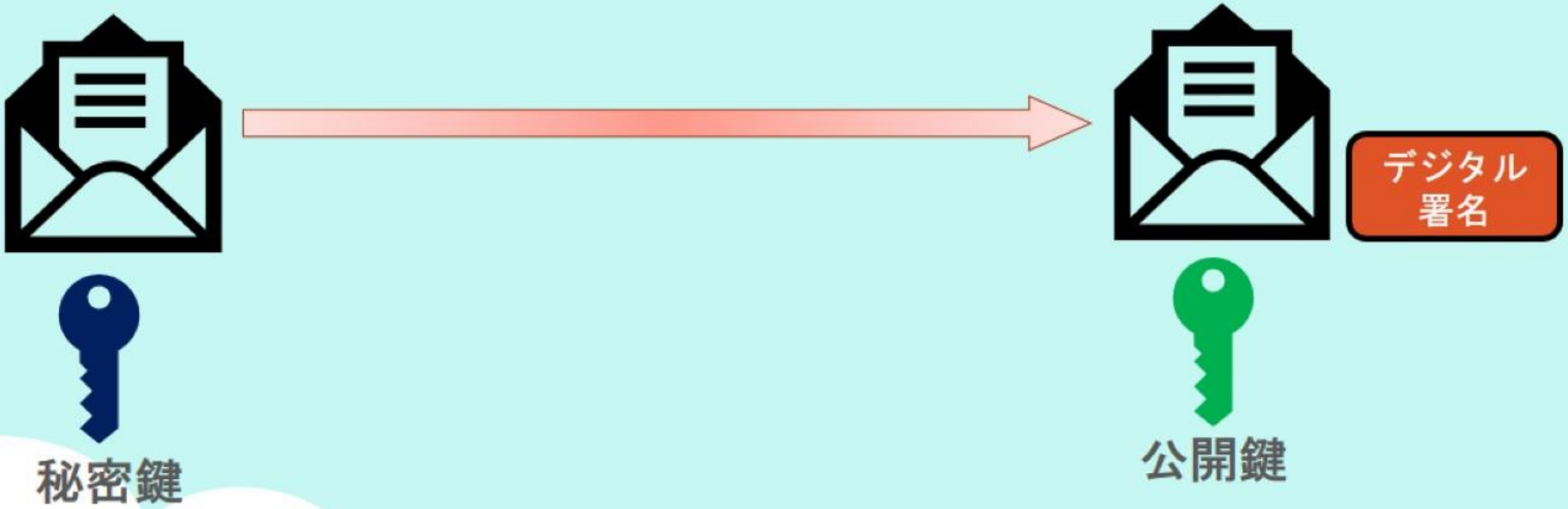
・デジタル署名



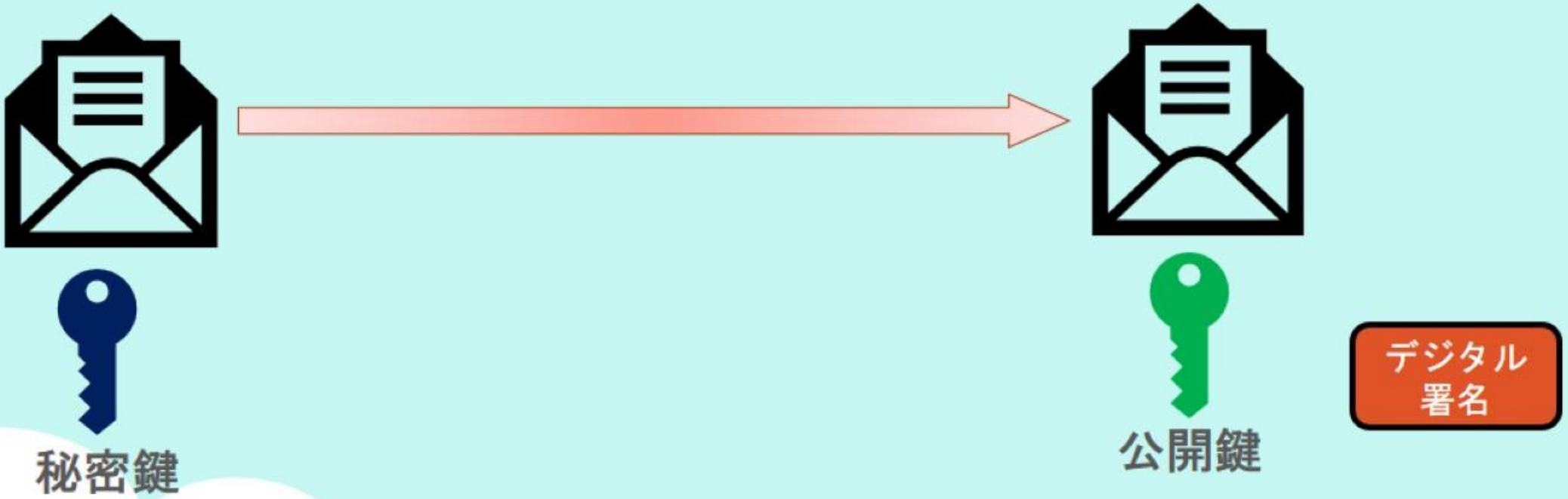
・デジタル署名



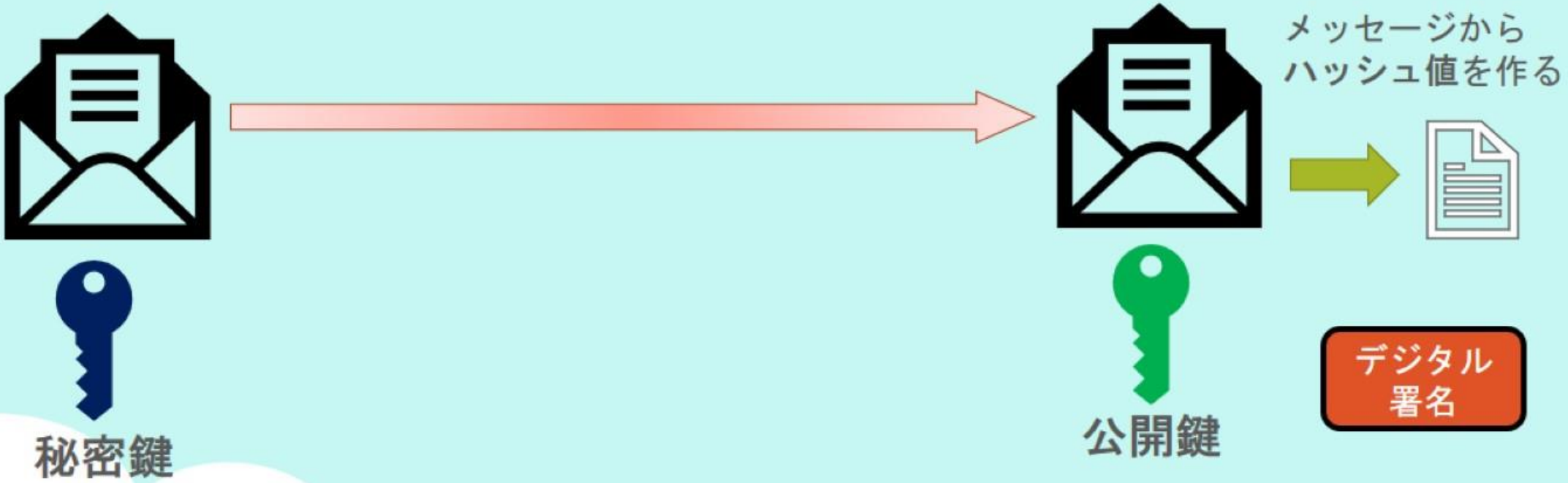
・デジタル署名



・デジタル署名

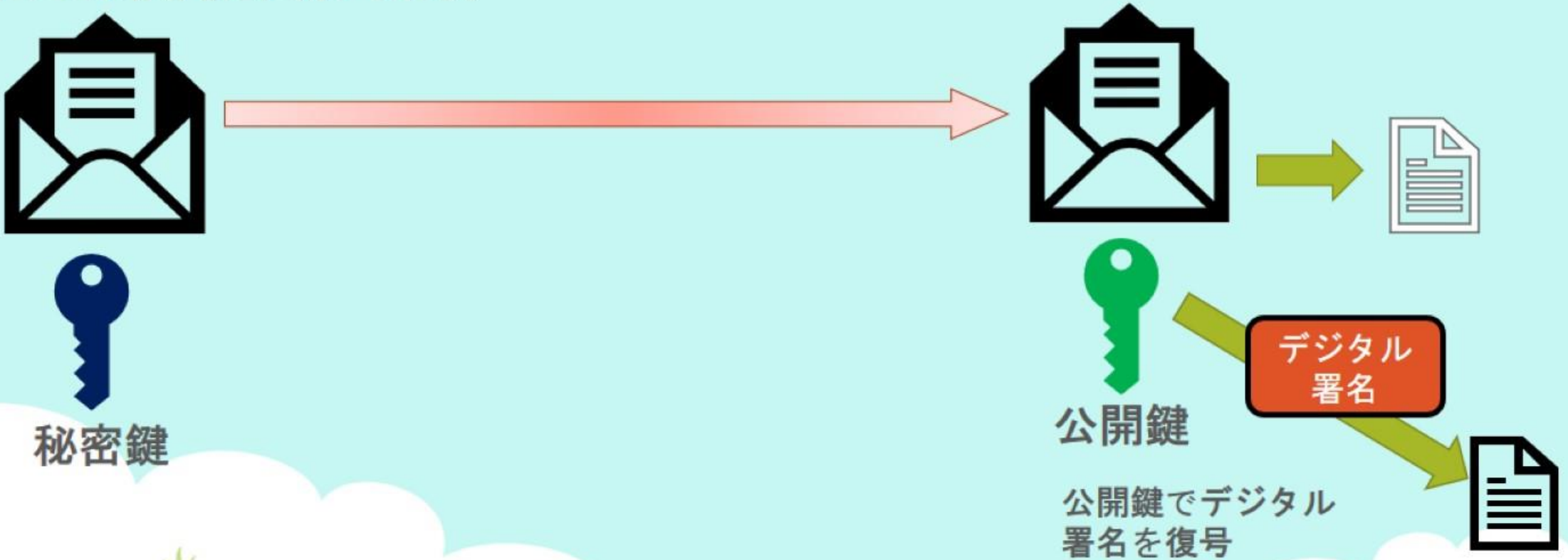


・デジタル署名

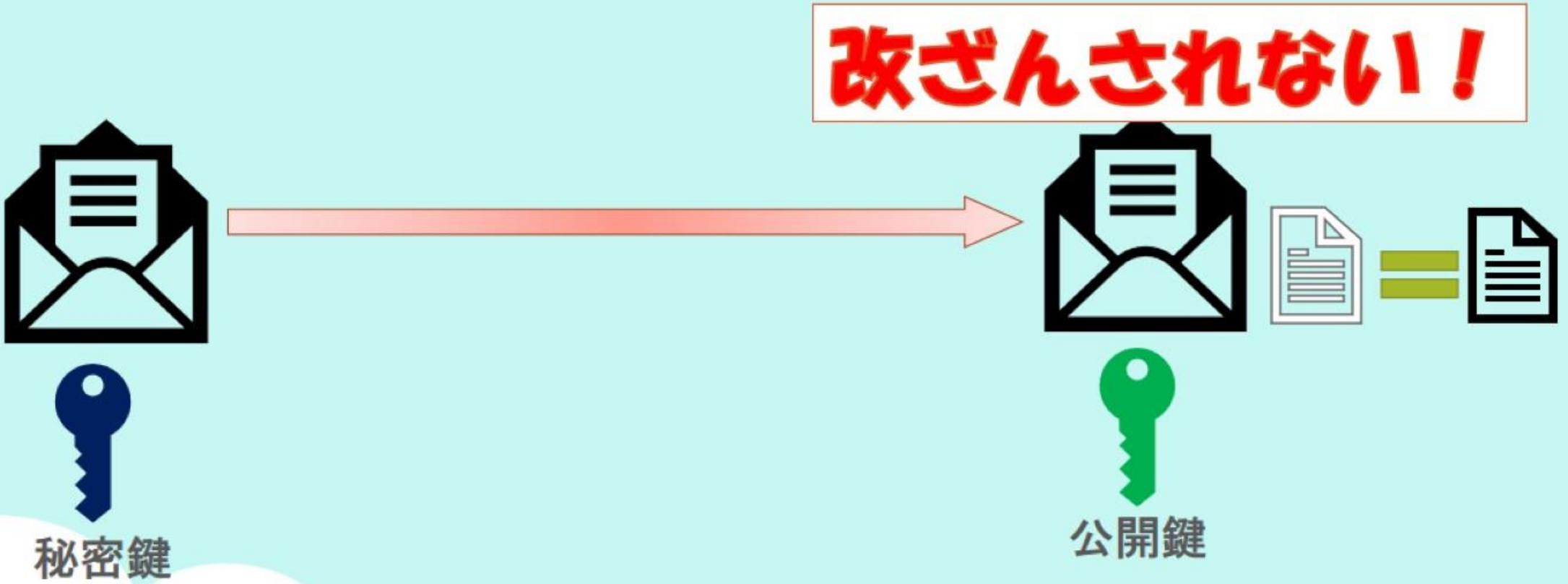


・デジタル署名

暗号技術を応用して、作られるハッシュ。
デジタル署名などに用いられる。



・デジタル署名



プログラムを作ってみよう