本文献について

- 本文献は下記論文を元にして作成されてものです。
  文書の内容の正確さは保証できないため、正確な知識を求める方は以下に示す原文を参照してください。

- 題目：暗号技術入門
- 著者：結城浩
- 発行者：新田光敏
- 初版発行：2008年12月10日
- 発行所：ソフトバンク クリエイティブ株式会社

暗号技術入門

名城大学 情報工学科
渡邊研究室
堀田直紀

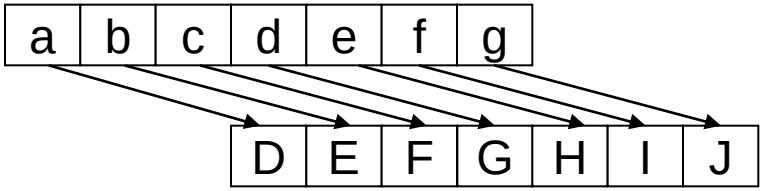
全体の流れ

- 暗号
  - 歴史上の暗号
  - 対称暗号(共通鍵暗号)
  - 公開鍵暗号
- 認証
  - 一方向ハッシュ関数
  - メッセージ認証コード
  - ディジタル署名
- PGP
- SSL/TLS

歴史上の暗号 1

シーザー暗号

- ジュリアス・シーザーが最初に使用
  - アルファベットを、一定文字数だけ「ずらす」作業を行う



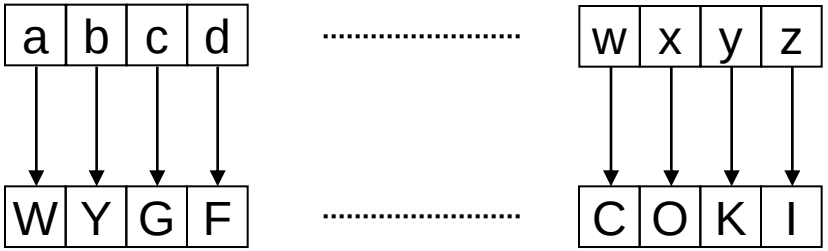
例：　平文 yoshiko　　暗号 BRVKLNR

- 問題点
  - 全数探索をすれば解読が可能になる

歴史上の暗号 2

単一換字暗号

- 平文を構成するアルファベットを別のアルファベットに変換する暗号



- 利点
  - 26の階乗の通り数があるため、解読することは困難
  - 1秒間に10億個の鍵を調べたとしてもすべての鍵を調べるのに、120億年以上の時間がかかる

歴史上の暗号 3

エニグマ

- シェルビウス(ドイツ)によって開発
  - 回転する円盤と電気回路を使用する
  - ナチスドイツ時代にドイツ国防軍に採用

- 暗号通信
  - エニグマを使って平文を暗号化し、エニグマを使って復号化
  - 送信者と受信者で同じ鍵を使用
  - 国防軍鍵表を使用
    - 日替わりの鍵が記されている

対称暗号1

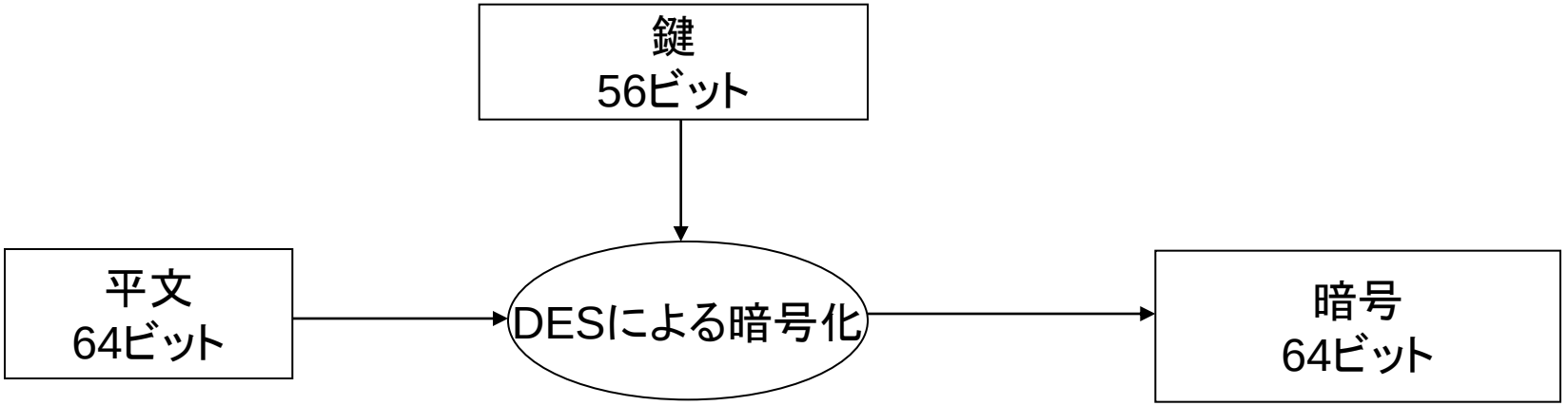
1つの鍵で暗号化し、同じ鍵で復号化する

- 使い捨てパッド
  - 平文と、ランダムなビット列とのXORをとる
  - 平文が64ビットの長さのビット列ならば、その長さと同じ64ビットのビット列が必要

- 問題点
  - 復号化の際、すべての64ビットのパターンが登場する
    ⇒ある文字列が復号されても、それが正しい平文なのか判定不能

対称暗号2

- DES
  - 64ビットの平文を一連の複雑な操作によって64ビットの暗号文に暗号化する
  - 鍵のビット長は56ビット
    - 7ビットおきにエラーの検出のための情報が1ビット入る



対称暗号3

- AES(Advanced Encryption Standard)
  - DESに代わっての新しい対称暗号アルゴリズム
  - アメリカ合衆国の標準化機関が公募
  - アメリカ合衆国の標準規格

名称	応募者
MARS	IBM社
RC6	RSA社
Rijndael	Daemen,Rijmen
Serpent	Anderson,Biham, Knudsen
Twofish	Counterpane社

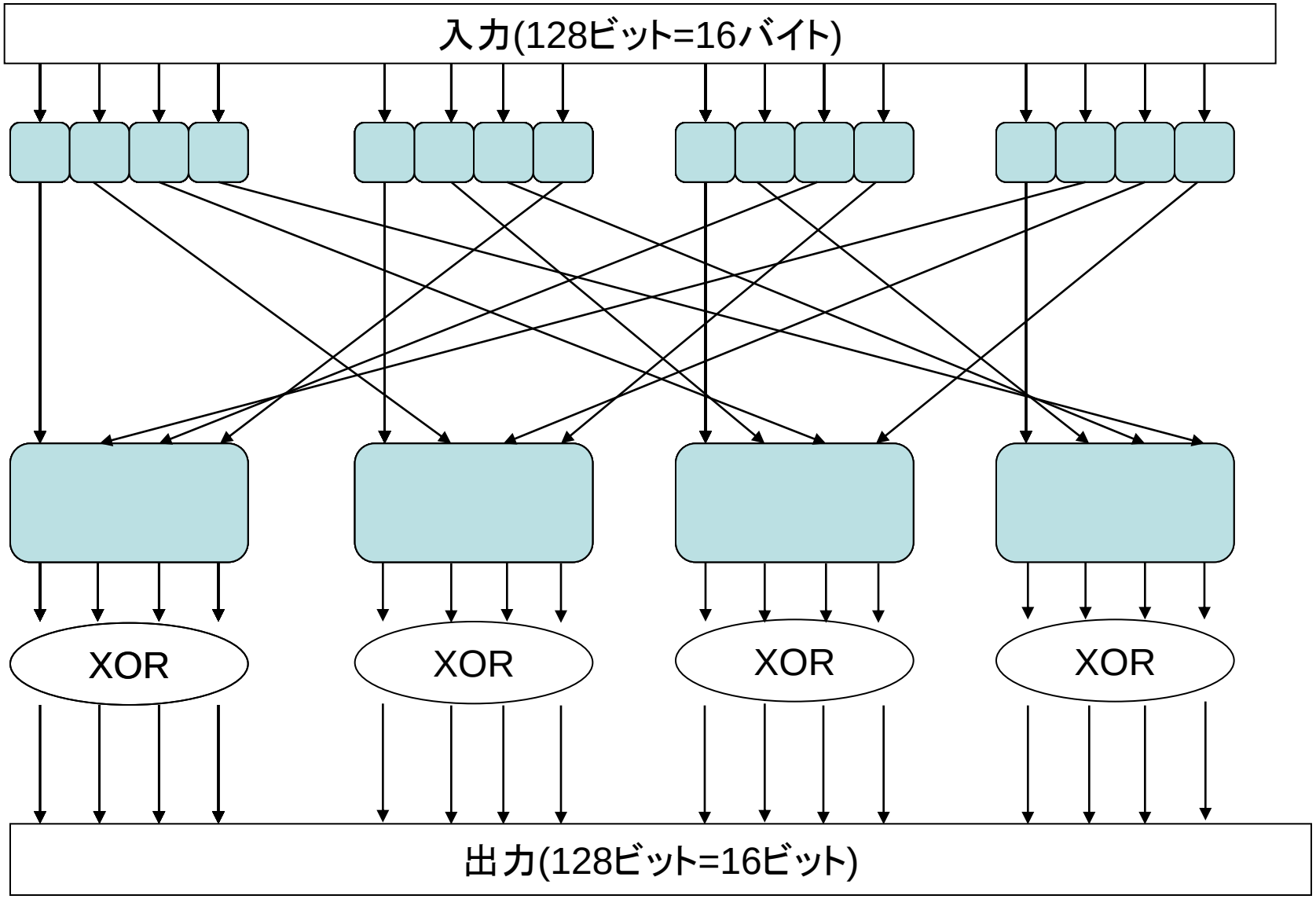
Rijndael

- ベルギーの研究者が設計
  - ブロック長は128ビット
  - 鍵のビット長は128ビットから256ビットまで32ビット単位で選択可能
  - ファイステルネットワークではなく、SPN構造という構造を使用

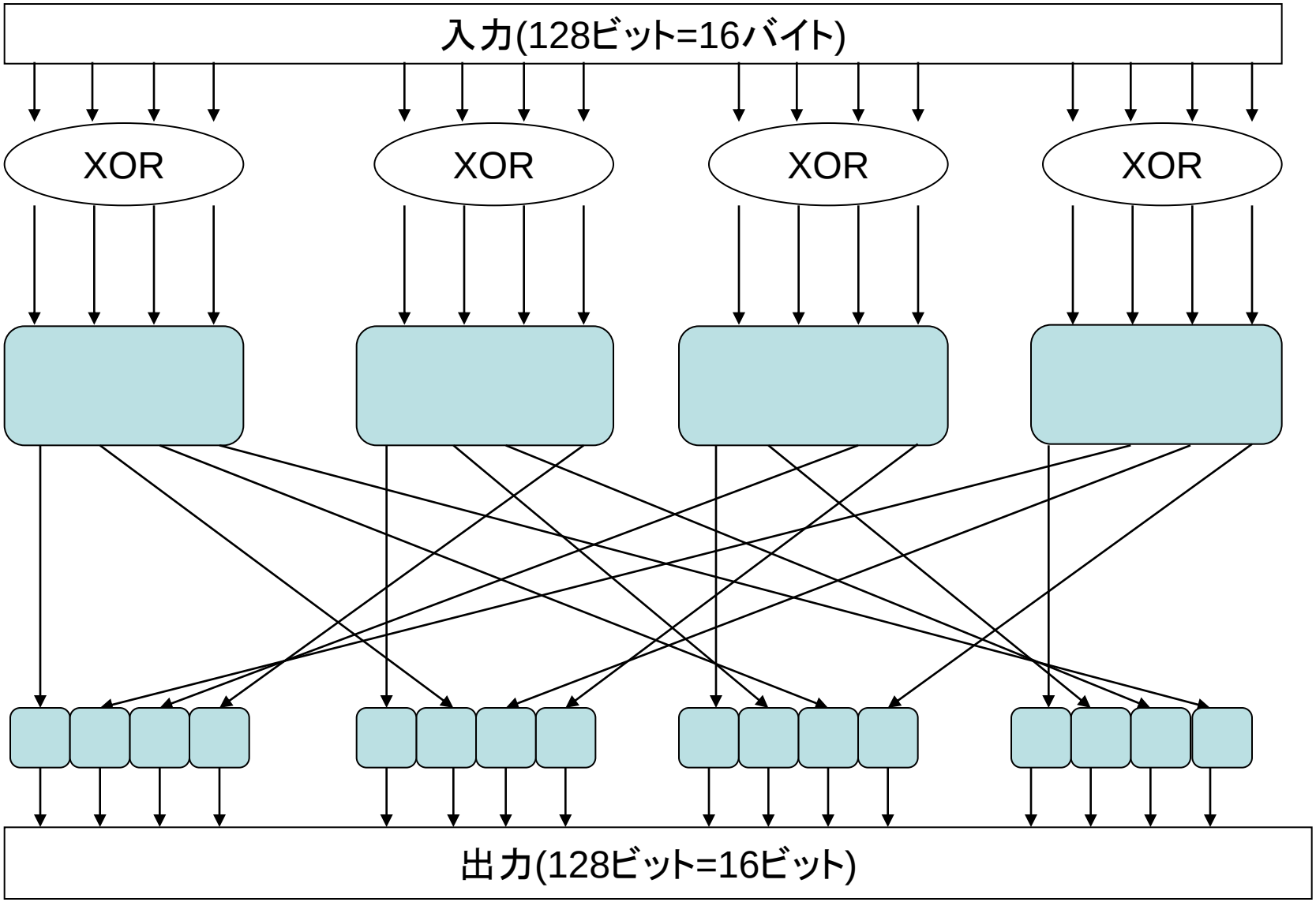
ファイステルネットワーク：繰り返し暗号の代表的な構成方法

SPN構造：3つの異なる同時置換

Rijndaelの暗号化



Rijndaelの復号化



公開鍵暗号

公開鍵で暗号化し、プライベート鍵で復号化する

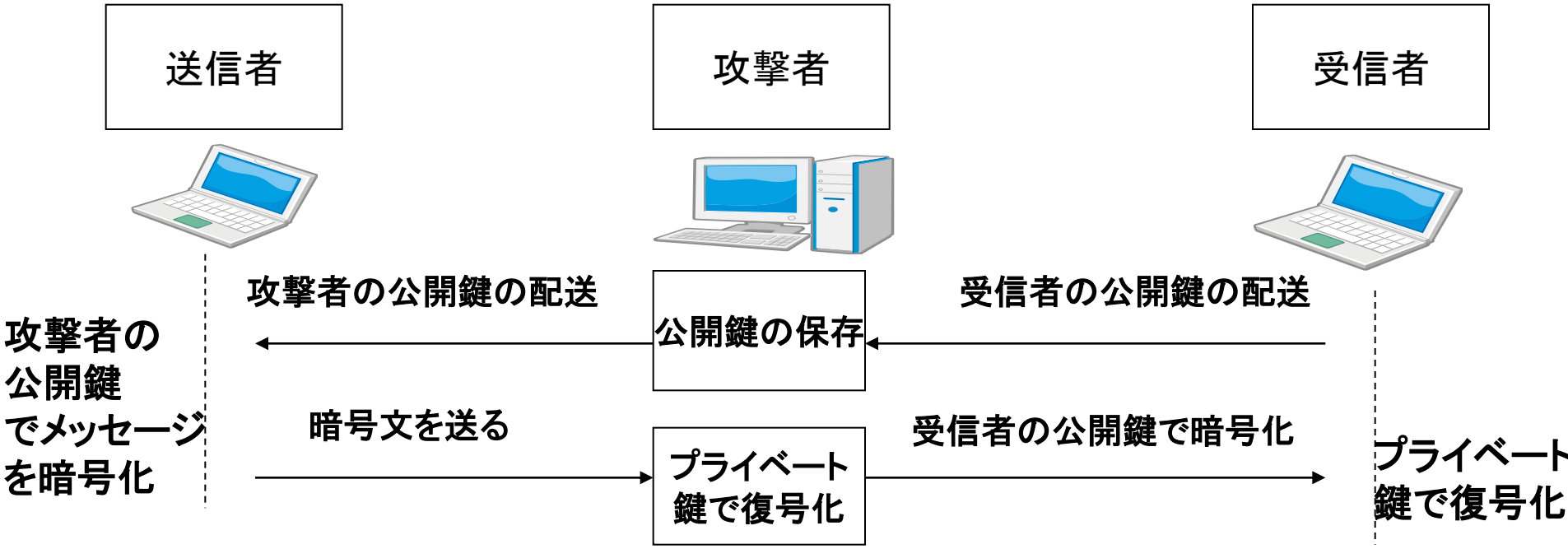
- 「暗号化の鍵」と「復号化の鍵」を分ける。
  ⇒鍵配送問題の解決

- 問題点
  - Man-in-the-middle攻撃
  - 公開鍵の認証

Man-in-the-middle攻撃

- 「間にいる人」という意味
- 送信者と受信者の間に能動的攻撃者が存在する
  - 攻撃者は公開鍵を改ざんしたり復号化することが可能

  ⇒公開鍵の証明書を用いる



他の公開鍵暗号

- ElGamal方式
  - mod Nで離散対数を求めるのが困難なことを利用している
- Rabin方式
  - mod Nで平方根を求めるのが困難なことを利用
- 楕円曲線暗号
  - 楕円曲線と呼ばれる曲線を定め、特殊な乗算をする

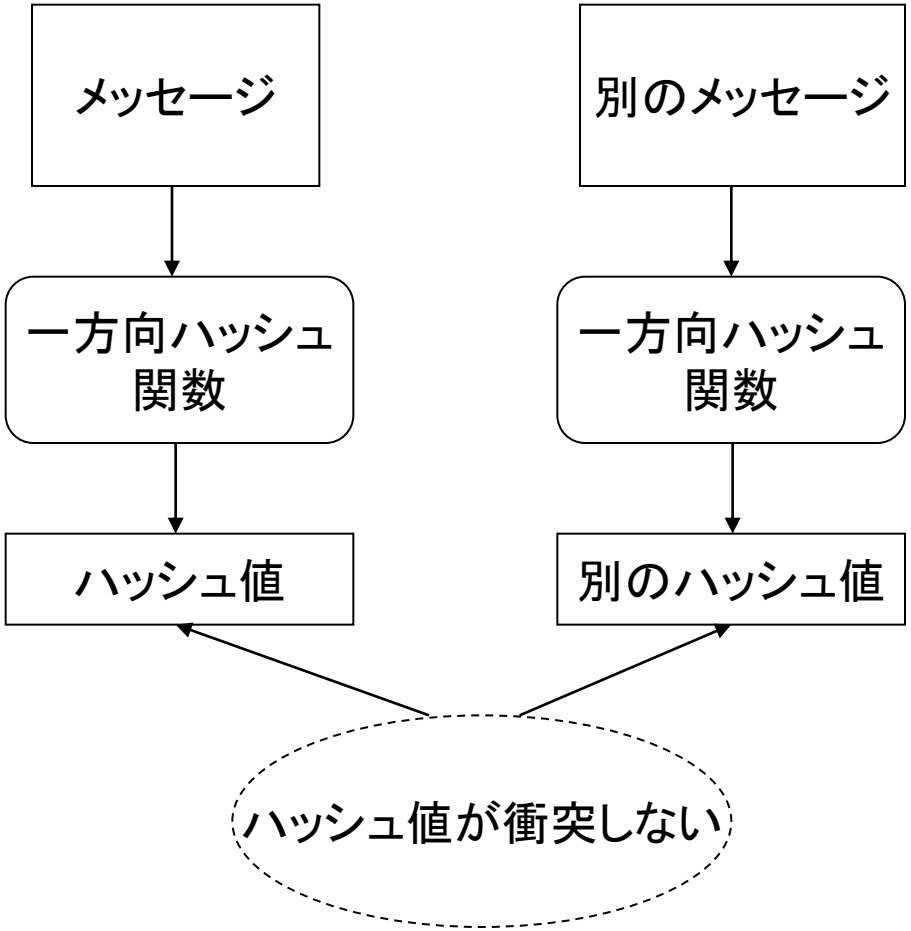
一方向ハッシュ関数

- メッセージの「指紋」をとる
- メッセージの正真性のチェックが可能

- 性質
  - 任意長のメッセージから固定長のハッシュ値を計算する
    - 利便性の向上
  - ハッシュ値を高速に計算できる
    - ハッシュ値を求めるための時間短縮
  - メッセージが異なればハッシュ値も異なる

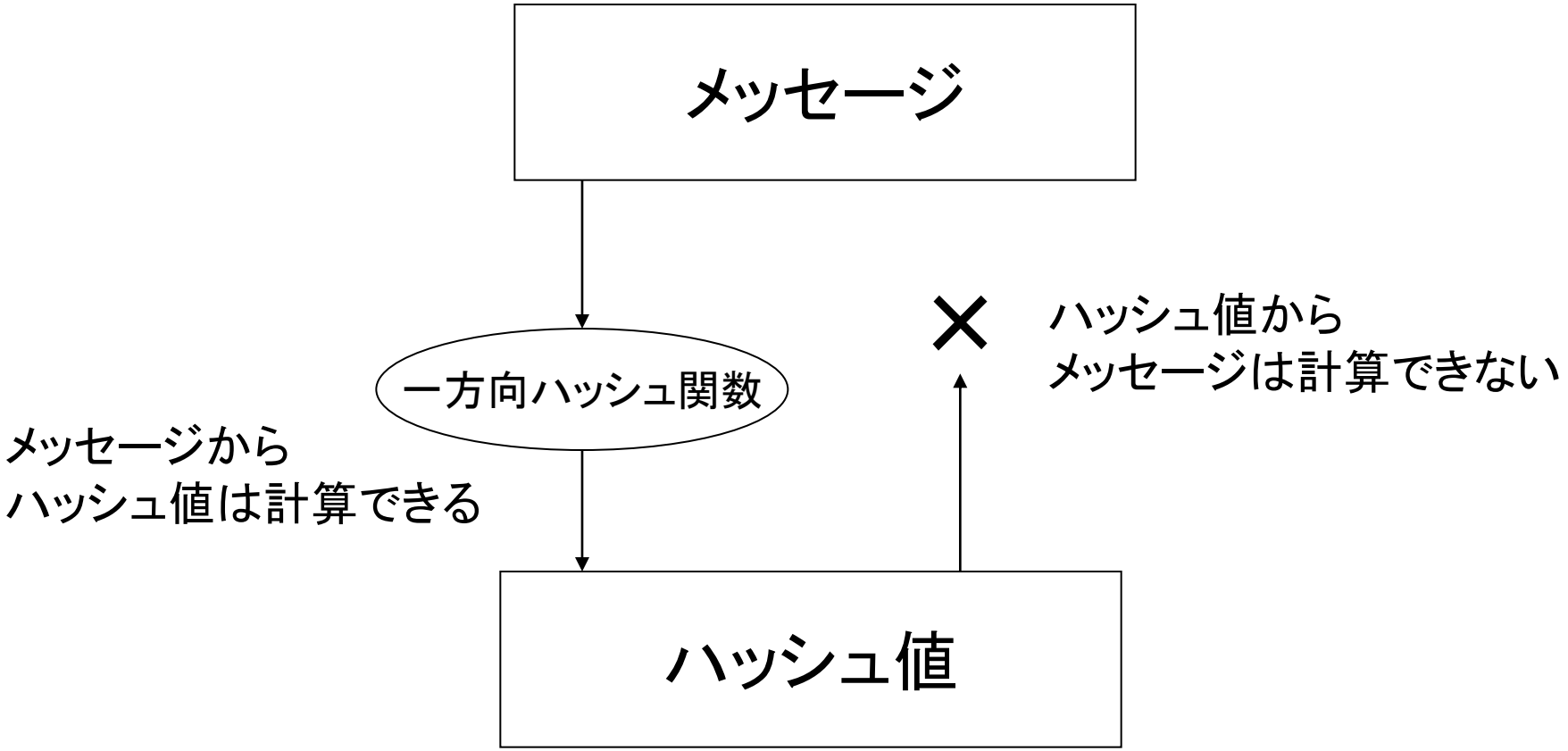
一方向ハッシュ関数

- 衝突耐性



一方向ハッシュ関数

- 一方向性を持つ
  - ハッシュ値からメッセージを逆算できない

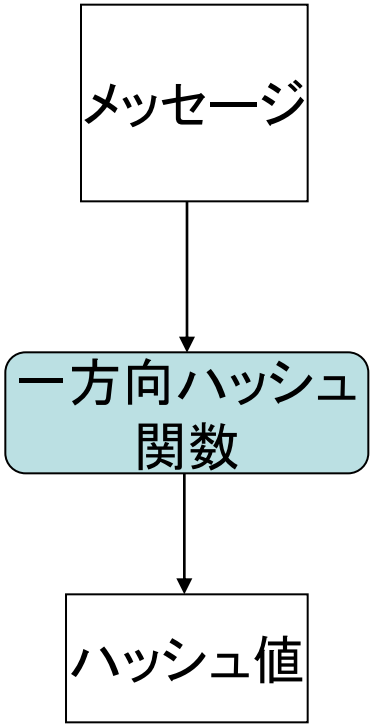


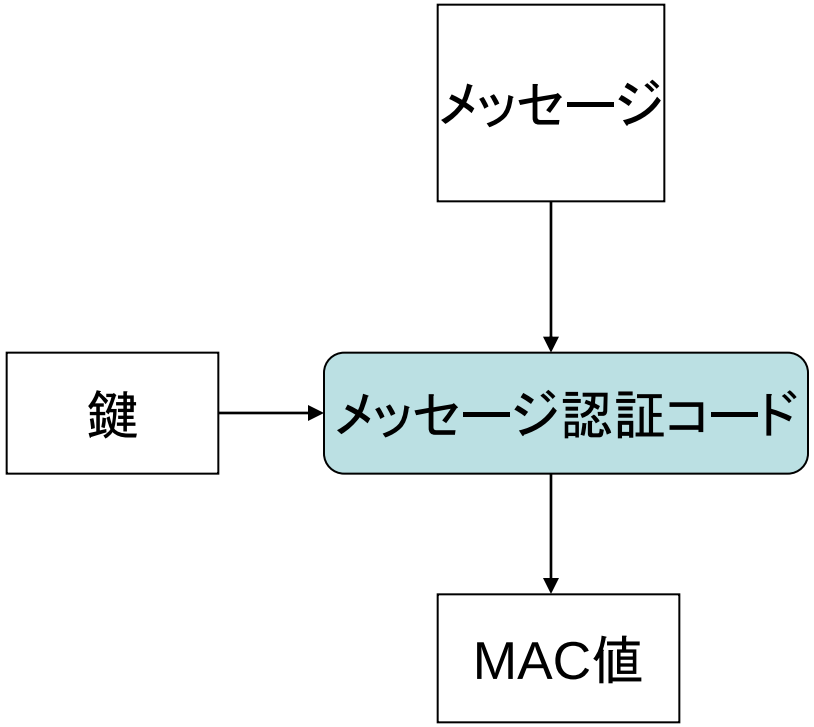
一方向ハッシュ関数の応用例

- メッセージ認証コード
  - 「送信者と受信者だけが共有している鍵」と「メッセージ」を混ぜ合わせ、そのハッシュ値を計算した値
- ソフトウェアの改ざん検出
  - 自分が入手したソフトウェアが改ざんされていないかを確かめる
- ワンタイムパスワード
  - 正当なクライアントであるかどうかをサーバが認証する

メッセージ認証コード

- 正真性を確認し、メッセージの認証を行う
  - 任意長のメッセージと、送信者と受信者が共有する鍵という2つの入力を元にして、固定ビット長の出力(MAC値)を計算する





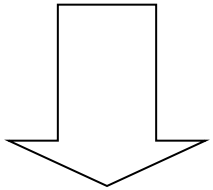
メッセージ認証コードの利用例

- SWIFT
  - 国際的な銀行間の送金を安全に行うために1973年に設立された団体
- IPsec
  - インターネットの根底をなす通信プロトコルのIP(Internet Protocol)にセキュリティの機能を加えたもの
  - 通信内容の認証と正真性のチェックに使用
- SSL/TLS
  - Webでオンラインショッピングを行うときなどに使用
  - 通信内容の認証と正真性のチェックに使用

デジタル署名

このメッセージを書いたのは誰か？

- 印鑑の捺印やサインに相当する機能をコンピュータの世界で実現するための技術
  - メッセージ送信時に送信者はプライベート鍵を使って署名を作成し、メッセージ受信時に受信者は別の鍵を使って署名を検証



  - 改ざんの検出、なりすましの検出、否認の防止が行える

証明書

自動車を運転するために必要な運転免許書のようなもの

- 公開鍵証明書
  - 名前や所属、メールアドレスなどの個人情報、その人の公開鍵が記載され、認証局によるデジタル署名が行われている

認証局：デジタル署名を作成できる人や組織のこと

PGP

- 1990年ごろにフィリップジマーマンという個人によって作成
- 極限状況の下に置かれた人のプライバシーを守ってきた暗号ソフトウェア

※「PGP-暗号メールと電子署名」『Garfinkel』

- 機能
  - 対称暗号
  - 公開鍵暗号
  - デジタル署名
  - 一方向ハッシュ関数
  - 証明書
  - 圧縮

SSL/TLS

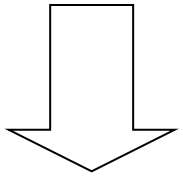
- 主にWebで利用される
  - インターネットのオンラインショップでクレジットカード番号を送信するときに使用
  - その際のURLは「http://」ではなく、「https://」となる


https://www.amazon.co.jp/gp/checkout/ship/select.html/ref=ox_shipoption_continue
支払い方法の選択
amazon.co.jp
サインイン 宛先 商品確認 ギフト 配送 会計 確認
支払い方法を選んでください
クレジットカードでお支払いの方へ:
• 指定したお届け先住所に初めて発送するため、カード情報の入力が必要です(カードでお支払いの場合のみ)
• 同じ住所にお届けする場合は、次回以降、入力する必要はありません
次に進む
(注文の最終確認ができます
カード以外の支払い方法
代金引換 国内配送のみ。お支払い後に注文がキャンセルされた場合や返品時にはAmazonギフト券での返金となります。ヘルプページ および 利用規約 をご確認ください。
コンビニ・ATM・ネットバンキング・ Edy払い(先払い) お客様に商品代金をお支払いいただいてからの商品発送となります。万が一お支払い後に注文がキャンセルされた場合や返品時にはAmazonギフト券での返金となります。ヘルプページおよび利用規約をご確認ください。
使用可能残高
Amazonポイント、Amazonギフト券、Amazonショッピングカード、キャンペーン用Amazonギフト券の使用可能残高がある場合に表示されます。支払い方法について 詳しくはこちら
新しいカードまたはギフト券で支払う
VISA
クレジットカード
カード情報を入力してください
カード番号
カード名義人(半角ローマ字) 有効期限
01
2010
クレジットカードの種類を選択
お客様のカード情報を追加
amazon.co.jp ギフト券
Amazonギフト券・Amazonショッピングカード または キャンペーン用Amazonギフト券
適用
ギフト券番号またはコードを入力(例: GIFT-SMPL12-XXXYYY)

SSL/TLSの注意点

- クレジット番号を送る相手として信用できるとは限らない

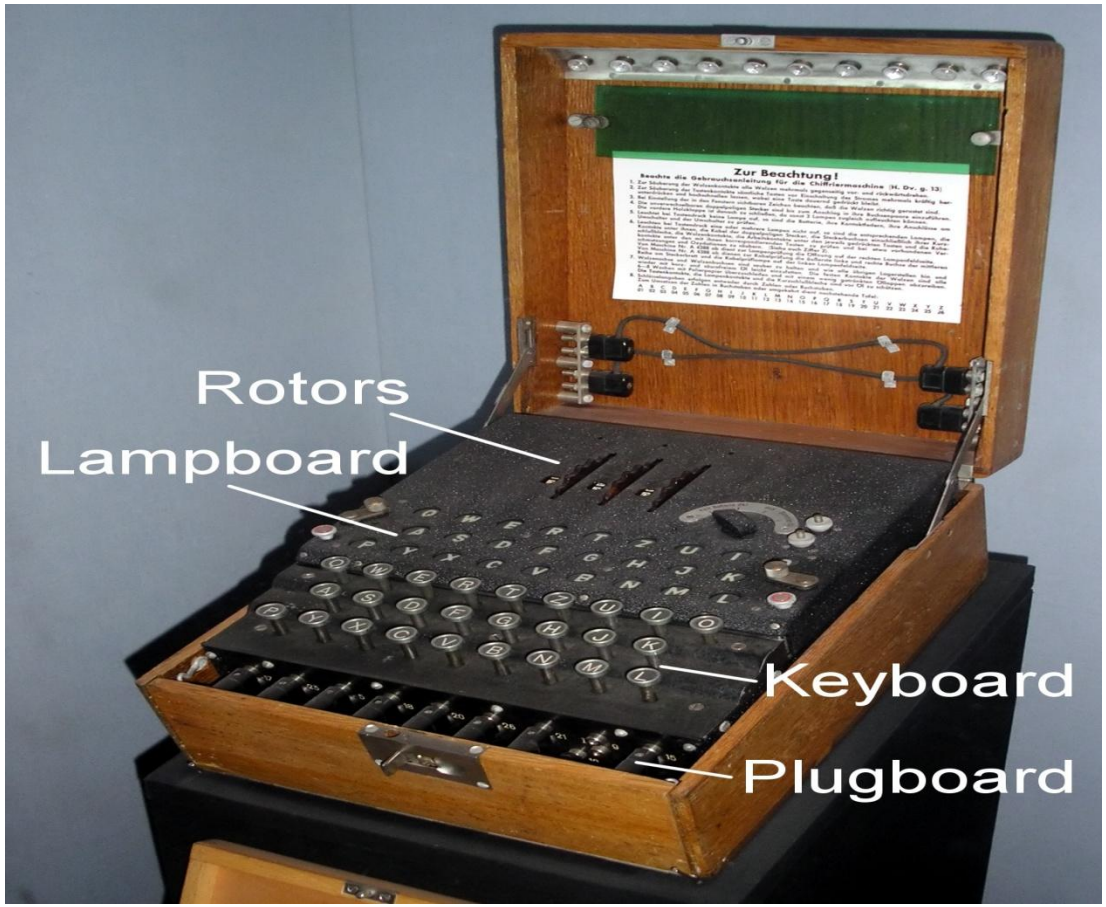
- 通信前、通信後のデータは守られていない
  - 個人情報を入力しているところを背後から覗き込まれたら・・
  - クレジット番号を送信した後の情報



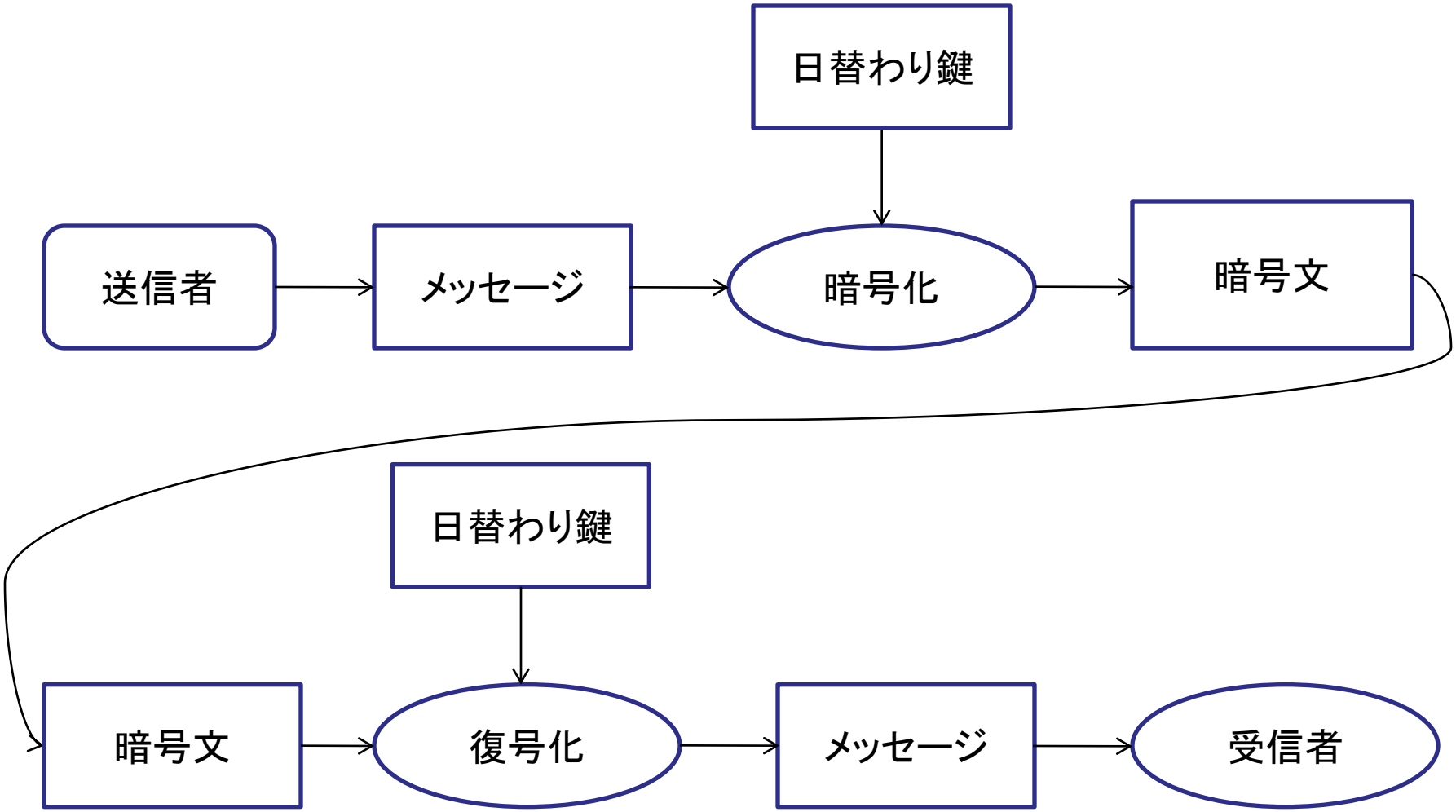
通信前、通信後に盗まれたり、悪用される危険性はある

以上

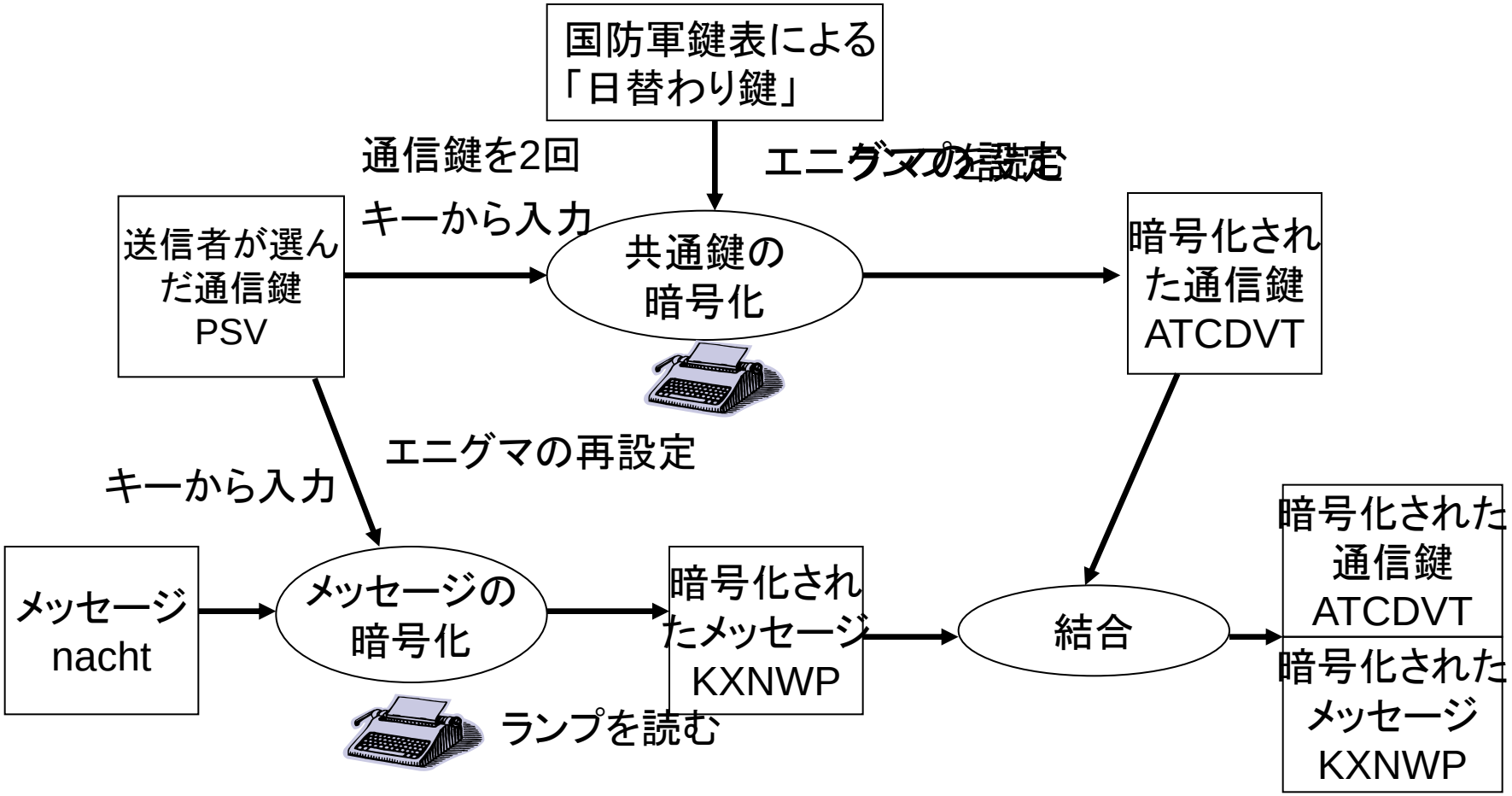
補足資料



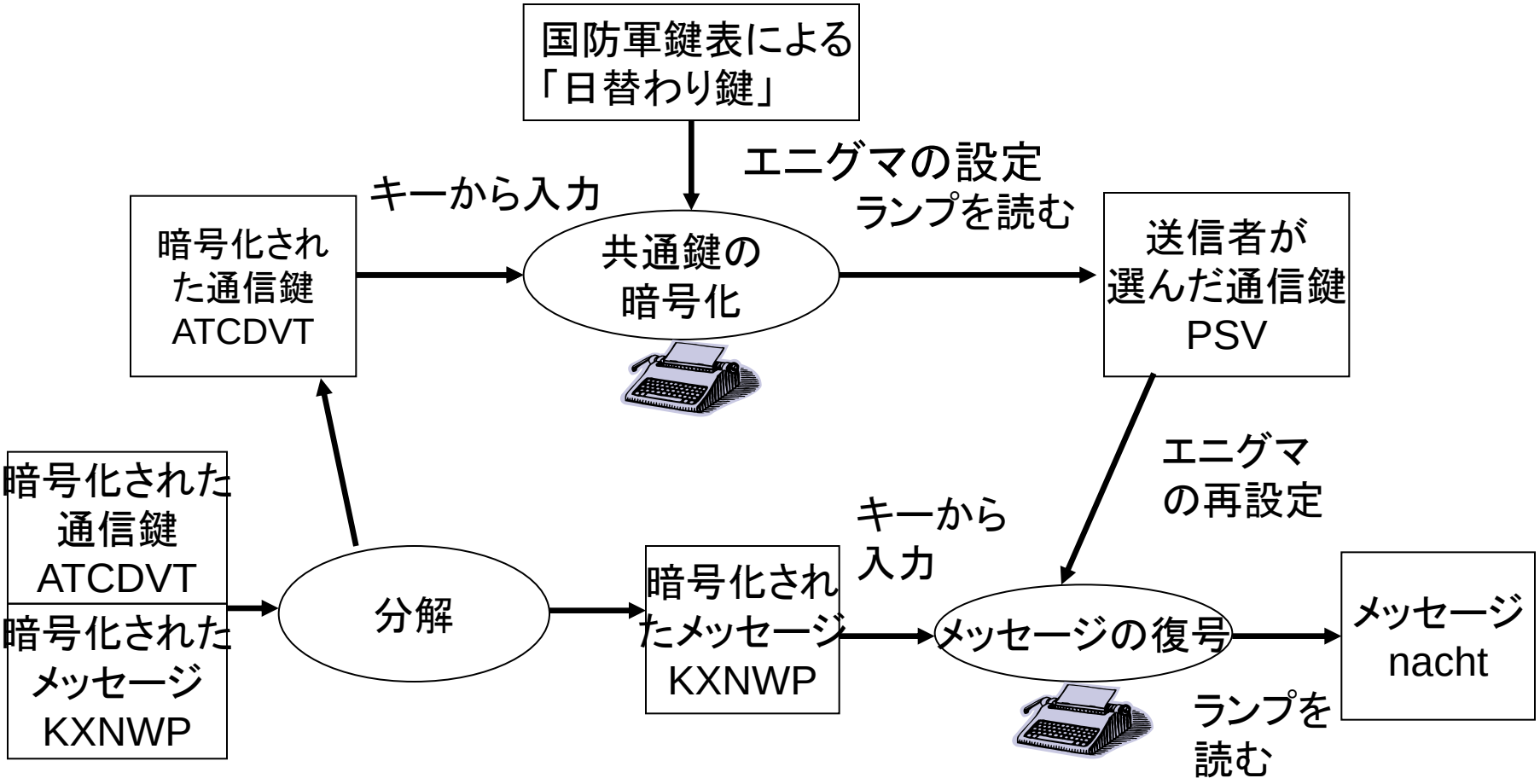
出展：フリー百科事典『ウィキペディア Wikipedia）』


日替わり鍵
送信者
メッセージ
暗号化
暗号文
日替わり鍵
暗号文
復号化
メッセージ
受信者

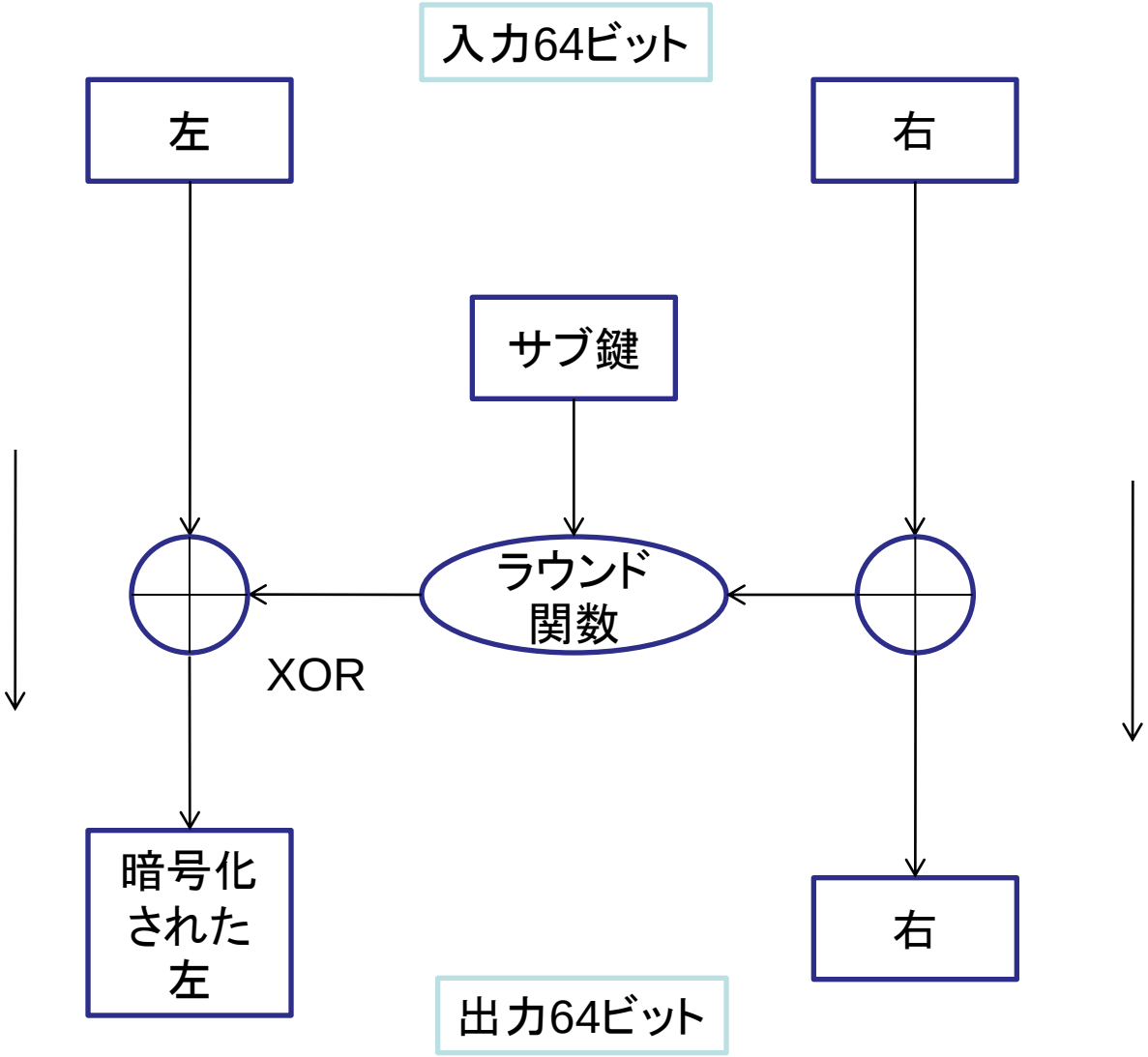
エニグマの暗号化


国防軍鍵表による
「日替わり鍵」
通信鍵を2回
キーから入力
エニグマの設定
送信者が選ん
だ通信鍵
PSV
共通鍵の
暗号化
暗号化され
た通信鍵
ATCDVT
エニグマの再設定
キーから入力
メッセージ
nacht
メッセージの
暗号化
暗号化され
たメッセージ
KXNWP
結合
暗号化された
通信鍵
ATCDVT
暗号化された
メッセージ
KXNWP
ランプを読む

エニグマの復号化


国防軍鍵表による
「日替わり鍵」
エニグマの設定
キーから入力
ランプを読む
暗号化された通信鍵
ATCDVT
共通鍵の
暗号化
送信者が
選んだ通信鍵
PSV
エニグマ
の再設定
暗号化された
通信鍵
ATCDVT
暗号化された
メッセージ
KXNWP
分解
暗号化され
たメッセージ
KXNWP
キーから
入力
メッセージの復号
メッセージ
nacht
ランプを
読む

ファイステルネットワークのラウンド

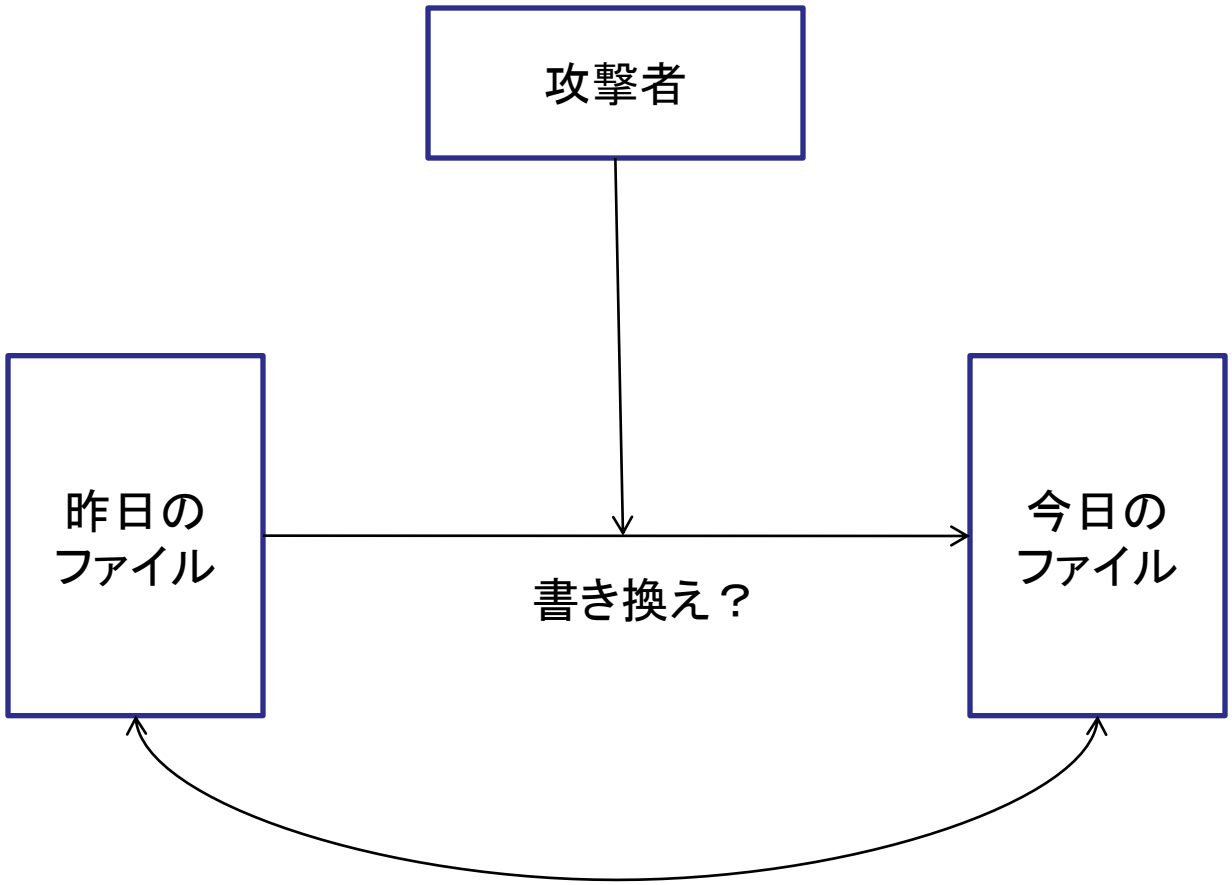


ハイブリッド暗号システム

- 対称暗号と公開鍵暗号の長所を生かすように組み合わせる
  - メッセージは、対称暗号で暗号化する
  - 対称暗号の暗号化で使うセッション鍵は、擬似乱数生成器で生成
  - セッション鍵は、公開鍵暗号で暗号化
  - 公開鍵暗号の暗号化で使う鍵は、ハイブリッド暗号システムの外部から与える

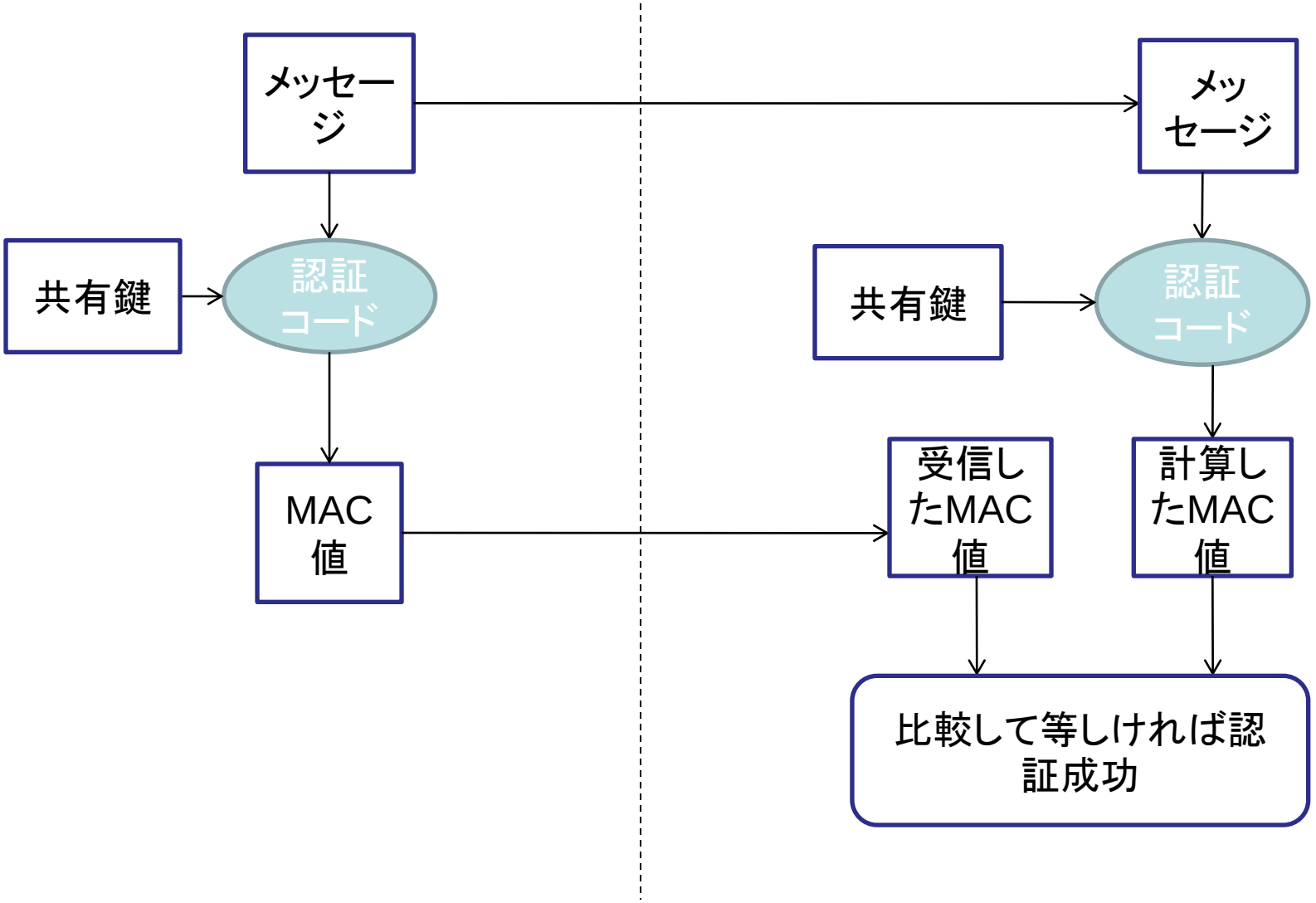
セッション鍵：今回の通信ためだけに一時的に作り出される鍵で擬似乱数器で生成させるもの

一方向ハッシュ関数



このニつは同じファイルか？？
（正真性の確認）

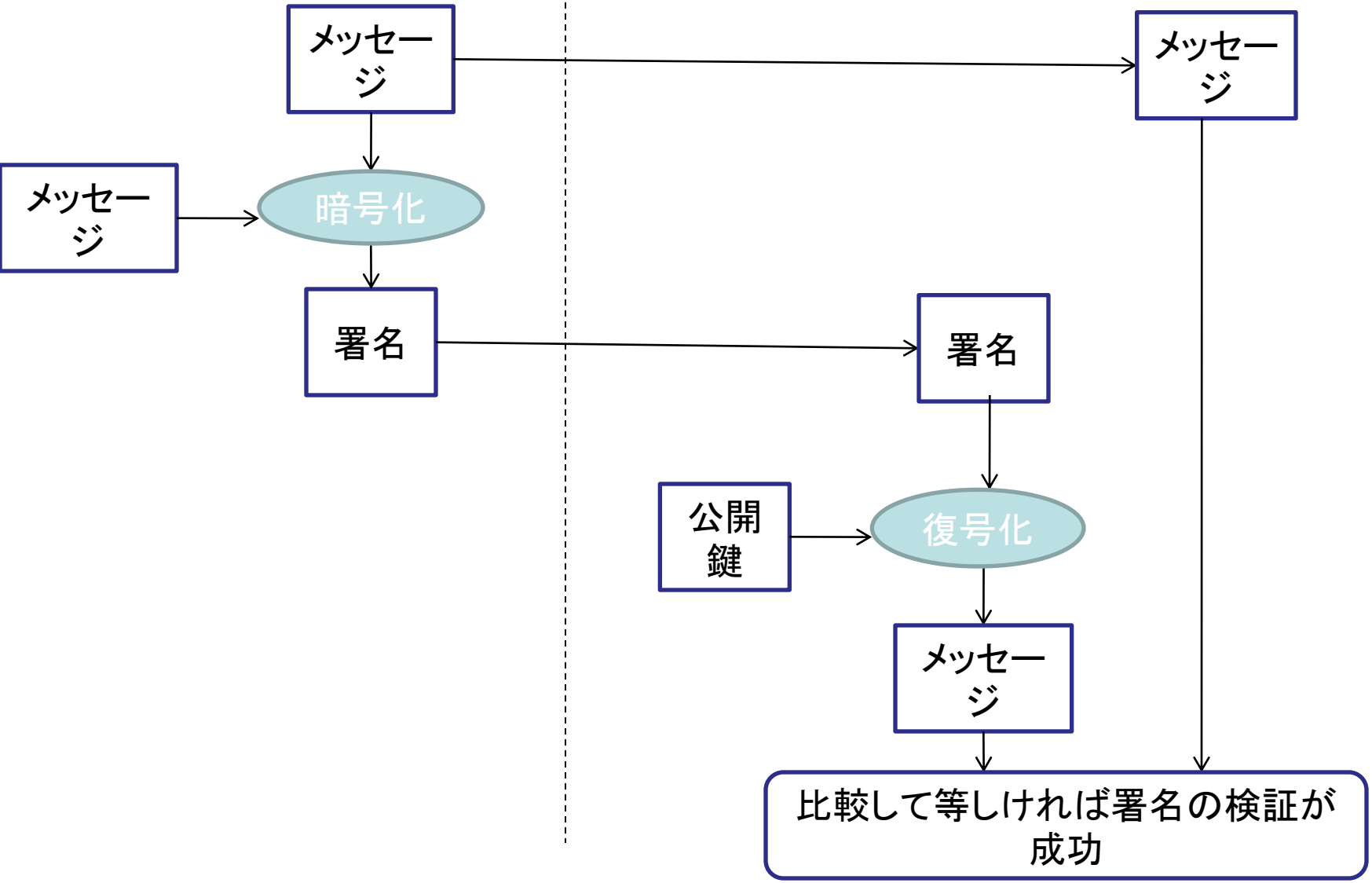
メッセージ認証コード


メッセージ
共有鍵
認証コード
MAC値
メッセージ
共有鍵
認証コード
受信したMAC値
計算したMAC値
比較して等しければ認証成功

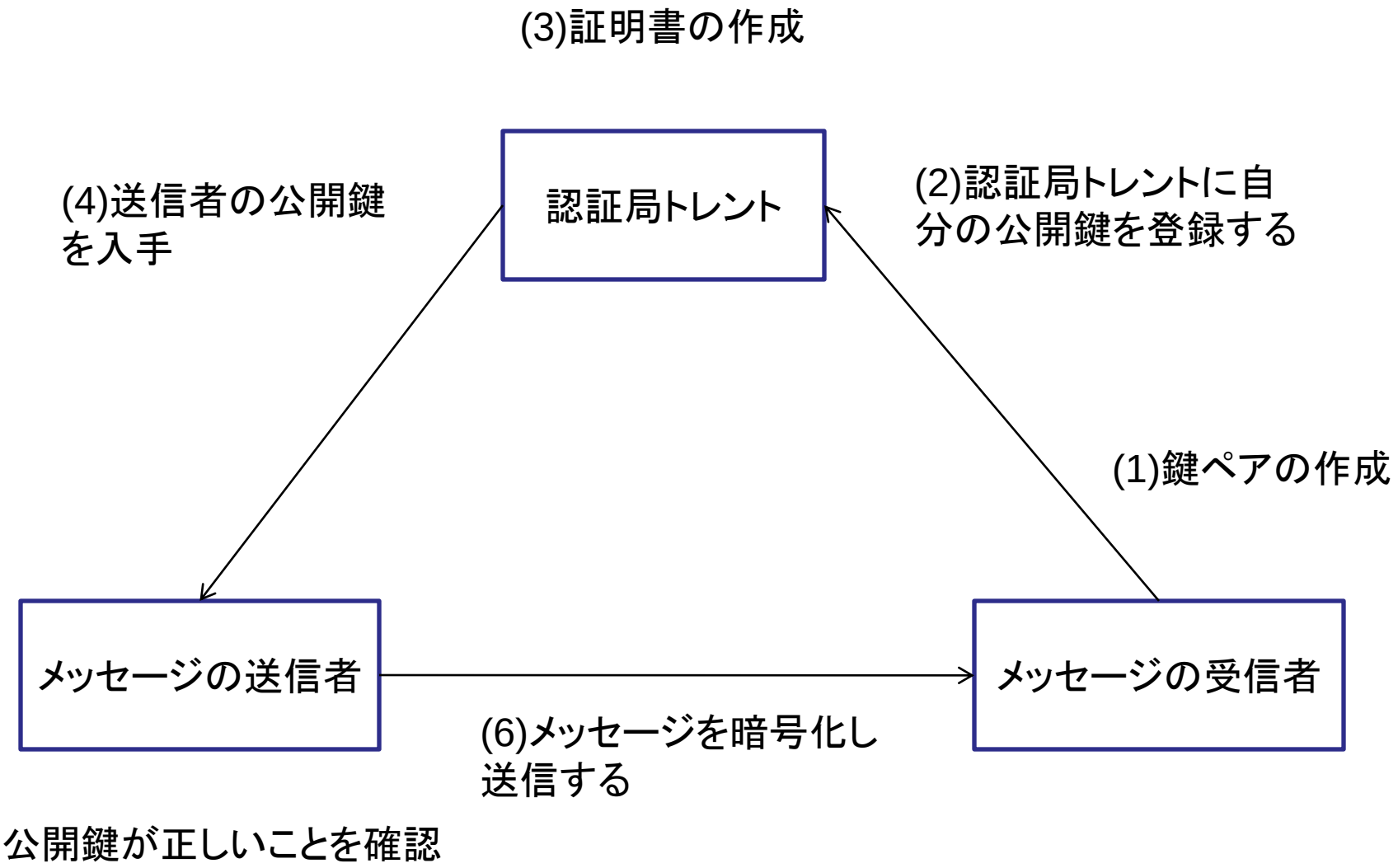
一方向ハッシュ関数の具体例

- MD4,MD5
  - 128ビットのハッシュ値を持つ
- RIPEMD-160
  - 160ビットのハッシュ値を持つ
  - RIPEMDの改訂版

ディジタル署名


メッセージ
メッセージ
メッセージ
暗号化
署名
署名
公開鍵
復号化
メッセージ
比較して等しければ署名の検証が成功

証明書


(3)証明書の作成
認証局トレント
(4)送信者の公開鍵
を入手
(2)認証局トレントに自
分の公開鍵を登録する
(1)鍵ペアの作成
メッセージの送信者
メッセージの受信者
(6)メッセージを暗号化し
送信する
(5)公開鍵が正しいことを確認