

情報セキュリティ特論

第2回

第2回：暗号と公開鍵暗号・認証および生体認証

今回の目標

- ・ 暗号の基礎および種類
- ・ 認証機構と生体認証

1. 暗号の基礎および種類

暗号技術

守秘

情報を隠す（他人に見られないようにする）こと

隠したい情報を「**暗号化**」することで達成

暗号化および復号のための「**鍵**」が必要

認証

情報が正しいことを検証すること

ログイン時のID/PW（なりすまし防止）

送信情報の改ざん防止

守秘

情報を隠す（他人に見られないようにする）こと
隠したい情報を「暗号化」することで達成
暗号化および復号のための「鍵」が必要



送信者

メール、文書ファイル



暗号化していないと傍受されてしまう



受信者



攻撃者

バーナム暗号

情報をBit(0か1)で表現し、鍵との排他的論理和 (XOR) を取る事で暗号化する

排他的論理和 (XOR)

A	B	$A \oplus B$	
1	1	0	AとBが同じ: 0
1	0	1	
0	1	1	
0	0	0	AとBが同じ: 0

バーナム暗号

情報をBit(0か1)で表現し、鍵との排他的論理和 (XOR) を取る事で暗号化する

排他的論理和 (XOR)

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

AとBが違う: 1

バーナム暗号

情報をBit(0か1)で表現し、鍵との排他的論理和 (XOR) を取る事で暗号化する

例) 4bitの平文をバーナム暗号で暗号化し、復号する

※暗号化の分野では原文のことを「平文」と言います。

暗号化

平文: 0 1 1 0

鍵: 1 0 1 1

暗号: 1 1 0 1

復号

暗号: 1 1 0 1

鍵: 1 0 1 1

平文: 0 1 1 0

XOR演算

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

バーナム暗号

情報をBit(0か1)で表現し、鍵との排他的論理和 (XOR) を取る事で暗号化する

例) 4bitの平文をバーナム暗号で暗号化し、復号する

※暗号化の分野では原文のことを「平文」と言います。

暗号化

平文: 0 1 1 0

鍵: 1 0 1 1

暗号: 1 1 0 1

復号

暗号: 1 1 0 1

鍵: 1 0 1 1

平文: 0 1 1 0

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

バーナム暗号で送ってみると



送信者

平文: 0 1 1 0

鍵: 1 0 1 1

暗号: 1 1 0 1



暗号: 1 1 0 1

暗号化と復号に同じ「鍵」が必要

鍵を安全に共有するには？



受信者

暗号: 1 1 0 1

鍵: 1 0 1 1

平文: 0 1 1 0

守秘

共通鍵暗号

公開鍵暗号

鍵共有

共通鍵暗号

暗号化と復号で同じ鍵を使う

ブロック暗号

ある一定の長さにブロック化して暗号化する方式

DES, 3-DES, AES

暗号の強さ: DES < 3-DES < AES

鍵の長さ: 56 56x3 256 (bit)

ストリーム暗号

一文字ずつ暗号化する方法

共通鍵暗号の問題点

送信者と受信者で鍵を共有することが必要

鍵が盗まれると終わり

鍵と暗号文の「総当たり」をされると暗号としての能力を失う

DESはもう安全では無い

3-DESも2023年には使用を停止することが提案されている

“Transitioning the Use of Cryptographic Algorithms and Key Length”,
NIST 800-131A, 208

公開鍵暗号

暗号化と復号で別の鍵を使う



鍵の共有が必要なくなる

公開鍵

秘密鍵



送信者



受信者

公開鍵の送信は復号に使えないので
傍受されても大丈夫



公開鍵

公開鍵の送信
(または取得)

秘密鍵

公開鍵

鍵ペアの生成

公開鍵暗号

暗号化と復号で別の鍵を使う



鍵の共有が必要なくなる

公開鍵 秘密鍵



送信者

暗号化された情報を送信



受信者

暗号
秘密鍵
平文

平文

公開鍵

暗号化

鍵を共有しなくて済む

秘密鍵

公開鍵

公開鍵暗号

公開鍵は傍受されても、秘密鍵があるので復号されない（されにくい）

方式:

RSA暗号

現在、もっともよく用いられる公開鍵の方式

素因数分解の困難さを利用して暗号の強度を確保している

（将来、素因数分解が瞬時にできるようになると安全ではなくなる）

ElGamal暗号

離散対数問題の困難さを利用して暗号の強度を確保している

2. 認証機構と生体認証

本人認証

「本人」であること如何に証明（担保）するか？

人間の場合

顔、声、体格、姿勢、立ち振る舞い

会話の内容、共通の話題、口癖

「振り込め詐欺」は上記の何も使っていない

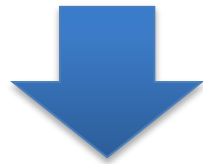
本人認証

- 顔、声、体格、姿勢、立ち振る舞い

生体認証（指紋、声紋、静脈）

- 会話の内容、共通の話題、口癖

パスワード、秘密の質問



では、これをもう少し正しく分類しましょう

多要素認証

個人を特定するには

唯一性、普遍性、固有性、を持つ情報が必要



固有情報を認証に使用

本人性・コスト

大



小

- A) 生体情報: 指紋、声紋、静脈
- B) 所持情報: ICカード、トークン
- C) 知識情報: パスワード、秘密の質問

「多要素認証」とはこれの組み合わせ

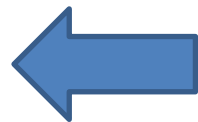
生体認証（バイオメトリック認証）

生体認証は個人の生体データを使う

指紋、網膜、虹彩、血管（静脈）、顔、音声、…

よって、認証を行うには

- 1) データ取得
- 2) 信号処理
- 3) 比較
- 4) 判定



この精度が認証の強さになる

のステップを踏むことになる。