分散システム 第12回
― セキュリティ ―

大連理工大学・立命館大学 国際情報ソフトウェア学部

大森 隆行

講義内容

- セキュリティ
  - 概説
    - セキュリティ特性、脅威、ポリシー
  - 暗号
  - 認証
  - 署名

情報セキュリティ

- セキュリティ特性 (セキュリティ3要素)
  - 機密性(Confidentiality)
    - システムが認可されたユーザに対してのみ情報を開示する
  - 完全性(Integrity)
    - システムの資産への改変が認可された方法でのみ行われる
    - 不当な改変は検知・修正する必要がある
  - 可用性(Availability)
    - 利用したいときに利用できるか
      (cf. フォールトトレラント性)
      → e.g., プロセス多重化、安定ストレージ

セキュリティ脅威

- 横取り(interception)：不正なデータアクセスが可能な状態
  - (例) ファイルシステムの個人ディレクトリが破られる
- 中断(interruption)：サービスやデータが利用不可能や無効になったり、破壊されたりする状態
  - (例) DoS攻撃(Denial of service)
- 改変(modification)：データの認められない変更、サービスの改竄
  - (例) データベース項目の改竄
- 合成(fabrication)：通常は存在しない付加的なデータやアクティビティが作られる状態
  - (例) 不正なアカウントの追加、不正なデータの追加

セキュリティポリシー

- セキュリティにも完璧はない
- システムにより、重要な箇所も異なる
- どのような脅威からどの程度守るべきかを明記
  → セキュリティポリシー
  - 何が許可／禁止されるべきか
- セキュリティメカニズム：セキュリティポリシーを実現するための仕組み
  - (例)
    暗号(encryption): 不正なユーザからデータを保護
    認証(authentication): 適切なユーザかを判断
    認可(authorization): 誰に何を許可するか
    監査(auditing): 誰が何をしたか記録を残して分析

確認問題

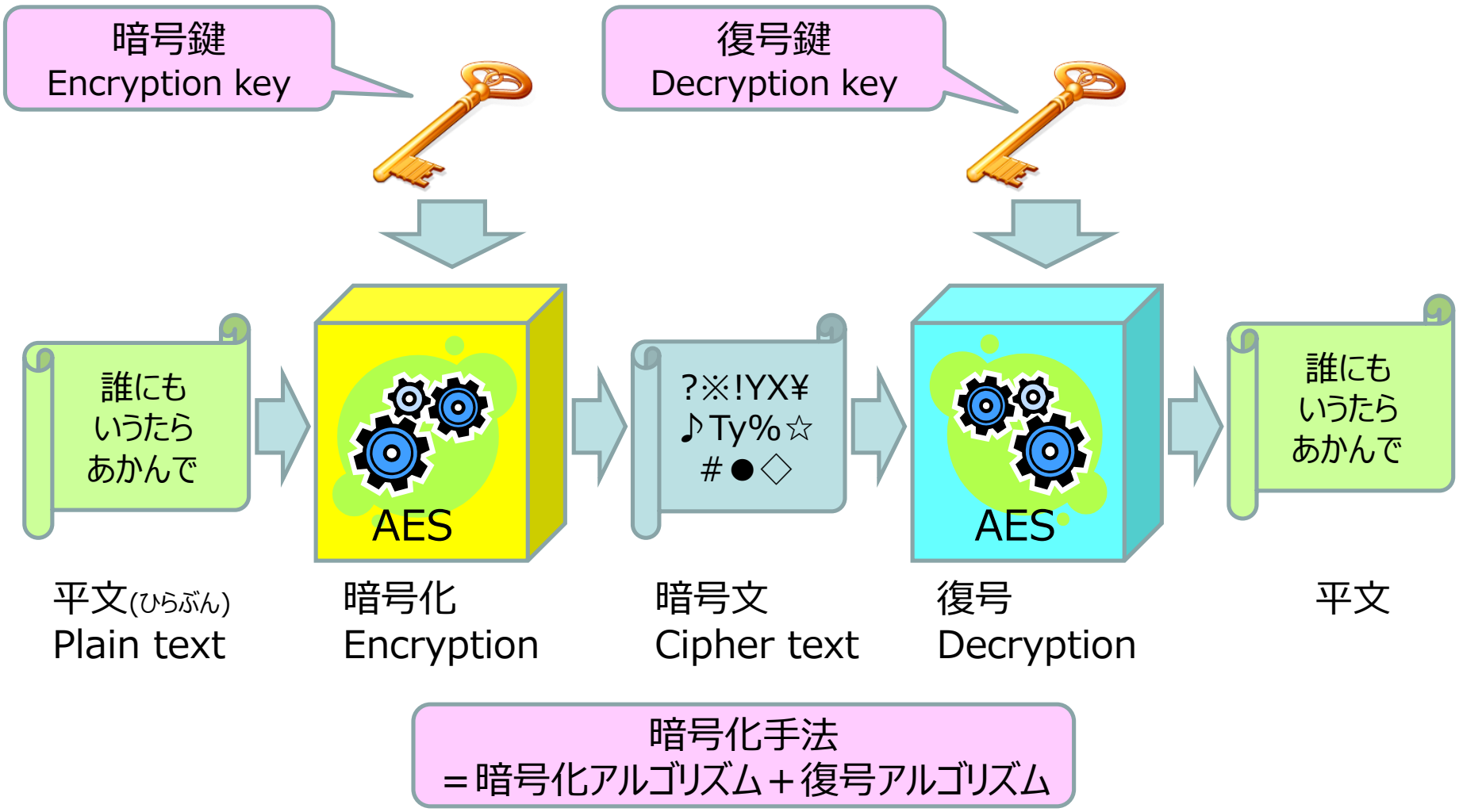
- セキュリティ特性として挙げられる3つの性質を挙げよ。
- 各文の説明に合うセキュリティ脅威の種類を語群から選んで答えよ。
  - データの認められない変更、サービスの改竄
  - 不正なデータアクセスが可能な状態
  - サービスやデータが利用不可能や無効になったり、破壊されたりする状態
  - 通常は存在しない付加的なデータやアクティビティが作られる状態

    語群：　横取り、中断、改変、合成
- システムのセキュリティ保持のため、どのような脅威からどの程度守るべきかを明記したものを何と呼ぶか。

講義内容

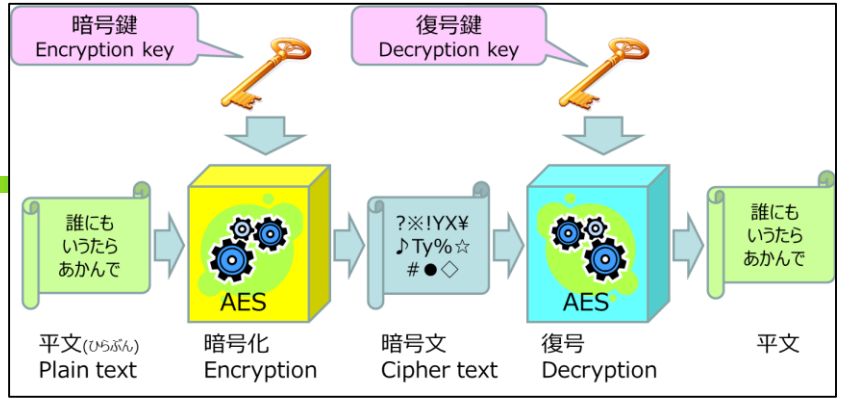
- セキュリティ
  - 概説
    - セキュリティ特性、脅威、ポリシー
  - 暗号
  - 認証
  - 署名

暗号化



暗号化手法
＝暗号化アルゴリズム＋復号アルゴリズム

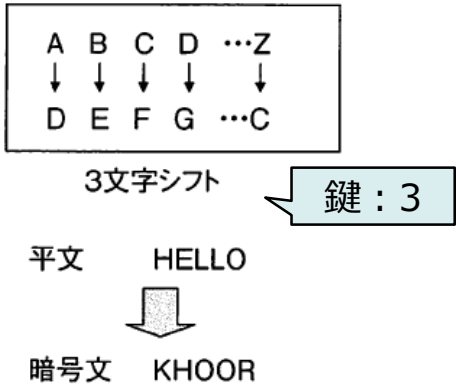
暗号化

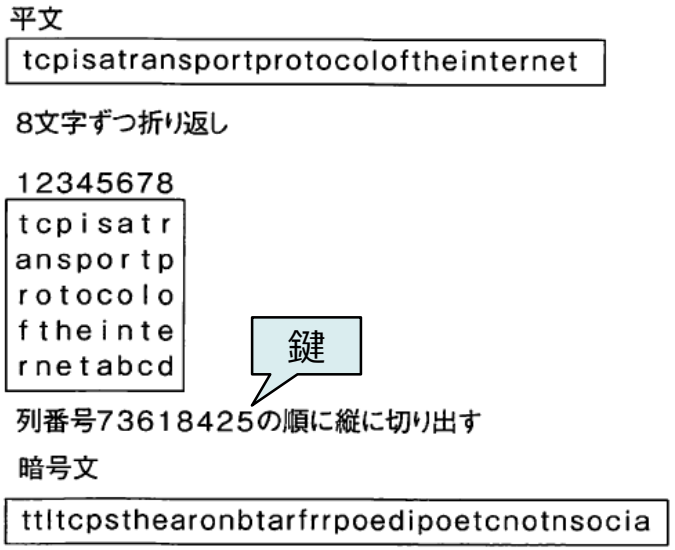


- 共通鍵暗号
  - 暗号鍵と復号鍵が同じ
  - 安全なルートで鍵を共有しなければならない
  - DES, 3DES, AES等のアルゴリズム
- 公開鍵暗号
  - 暗号鍵は公開されている。復号鍵は非公開(秘密)
    (暗号鍵と復号鍵は異なる)
  - 公開鍵から秘密鍵を推測するのは不可能 or
    莫大な計算量を要する
  - 公開鍵で生成された暗号文は、対になる
    秘密鍵でしか復号できない
  - 暗号文から公開鍵や秘密鍵が推測できない
  - RSA, DSA等のアルゴリズム

暗号の種類

- 換字式暗号
  - 平文の文字を異なる文字に決まった方法で置き換える方式
  - (例) シーザー暗号
- 転置式暗号
  - 平文の文字の場所を決まった法則で入れ替える方式





秘密分散

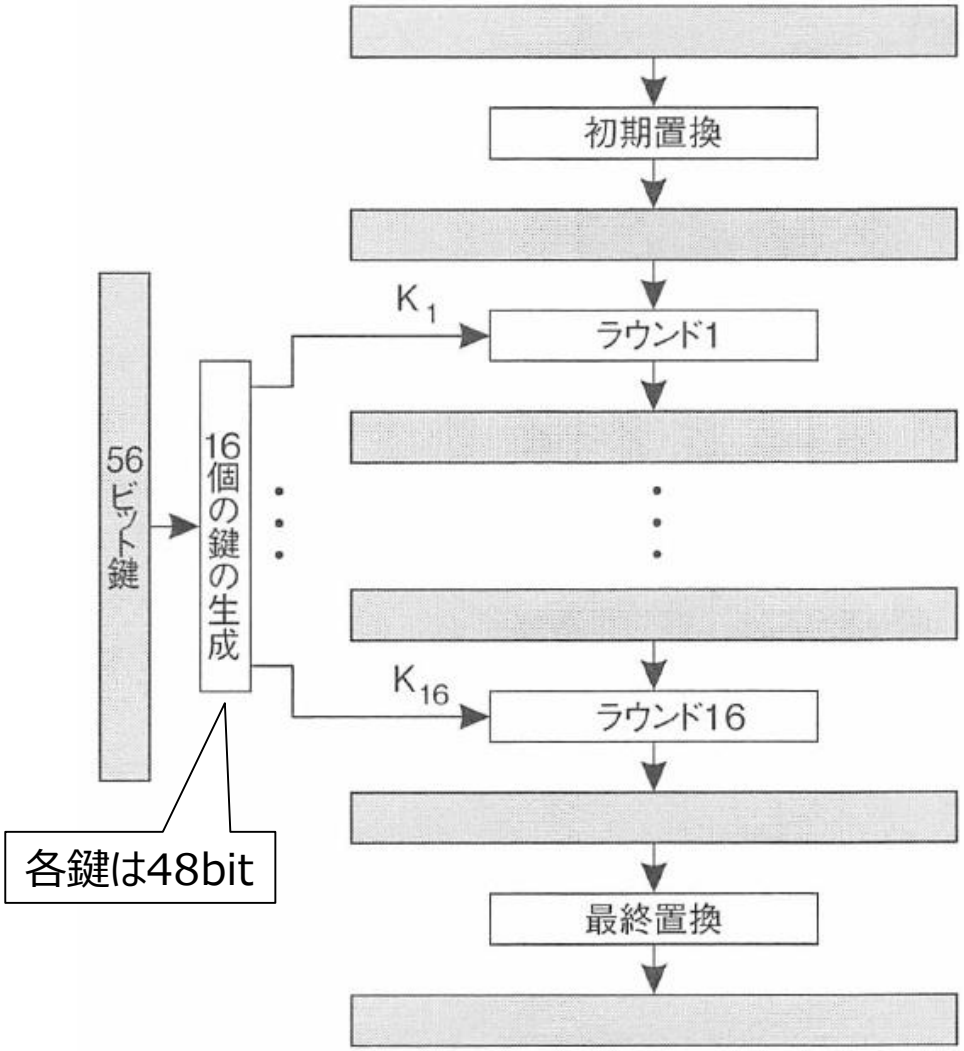
- 秘密にしておきたい情報をいくつかの情報(シェア)に分割する
- シェアを一定数以上集めると元の情報が得られる

- (例) F(X)=aX+S
  - S：秘密情報、a：適当な定数
  - N人の参加者のうちi番目の人にF(i)の値を配布
  - 仮に F(1)=2 だと分かっても、a,Sを逆算できない
  - F(1)=2, F(2)=3 だと分かるとa=1, S=1 だと逆算可能
    - ⇨ N人のうち2人の情報を集めると元の情報が得られる

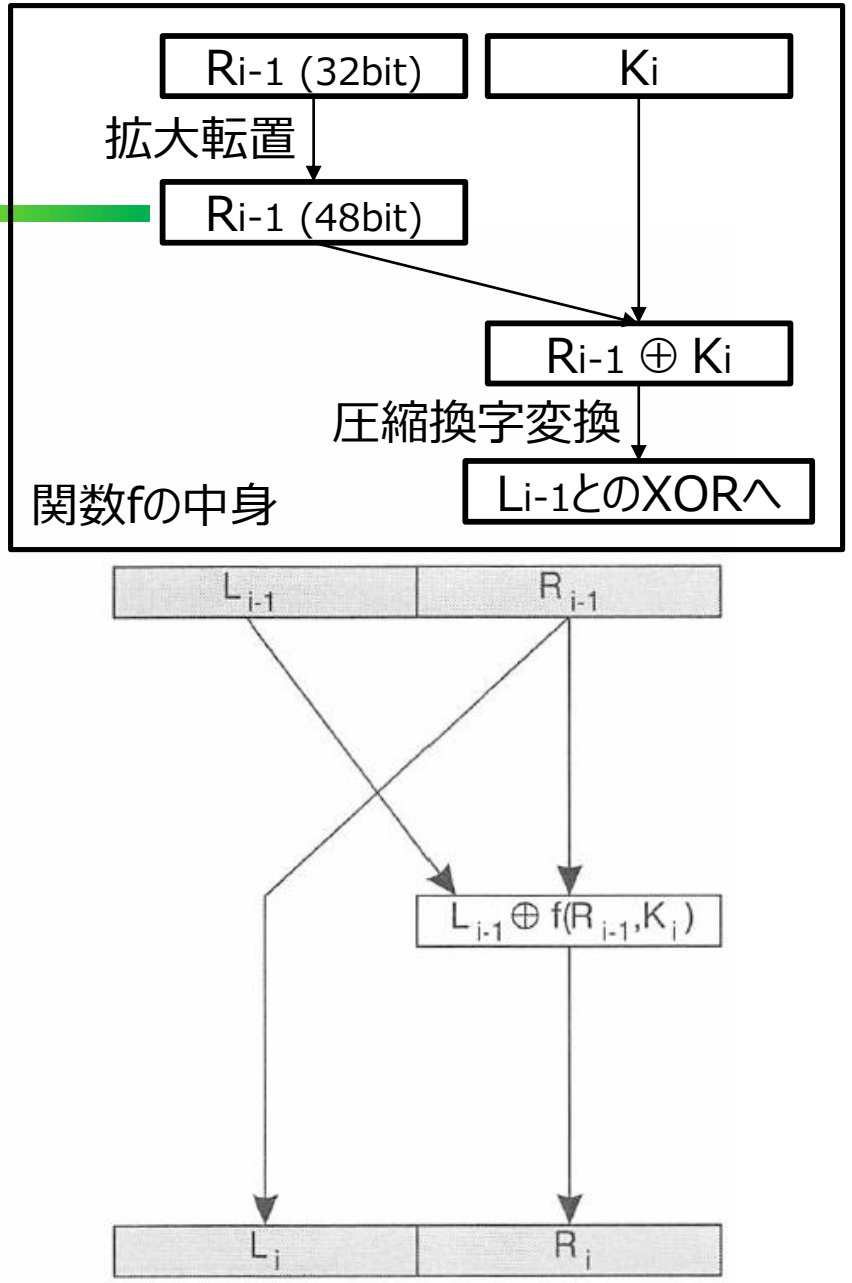
DES (Data Encryption Standard)

- 共通鍵暗号方式
- ブロック暗号
  - 情報をブロックと呼ばれる一定長の
    まとまりごとに処理
  - 平文64ビット→暗号文64ビット
- 鍵の長さは56ビット
  (+8ビットのパリティビット)
- 16段階の反復処理(＋前処理・後処理)で暗号化

DES



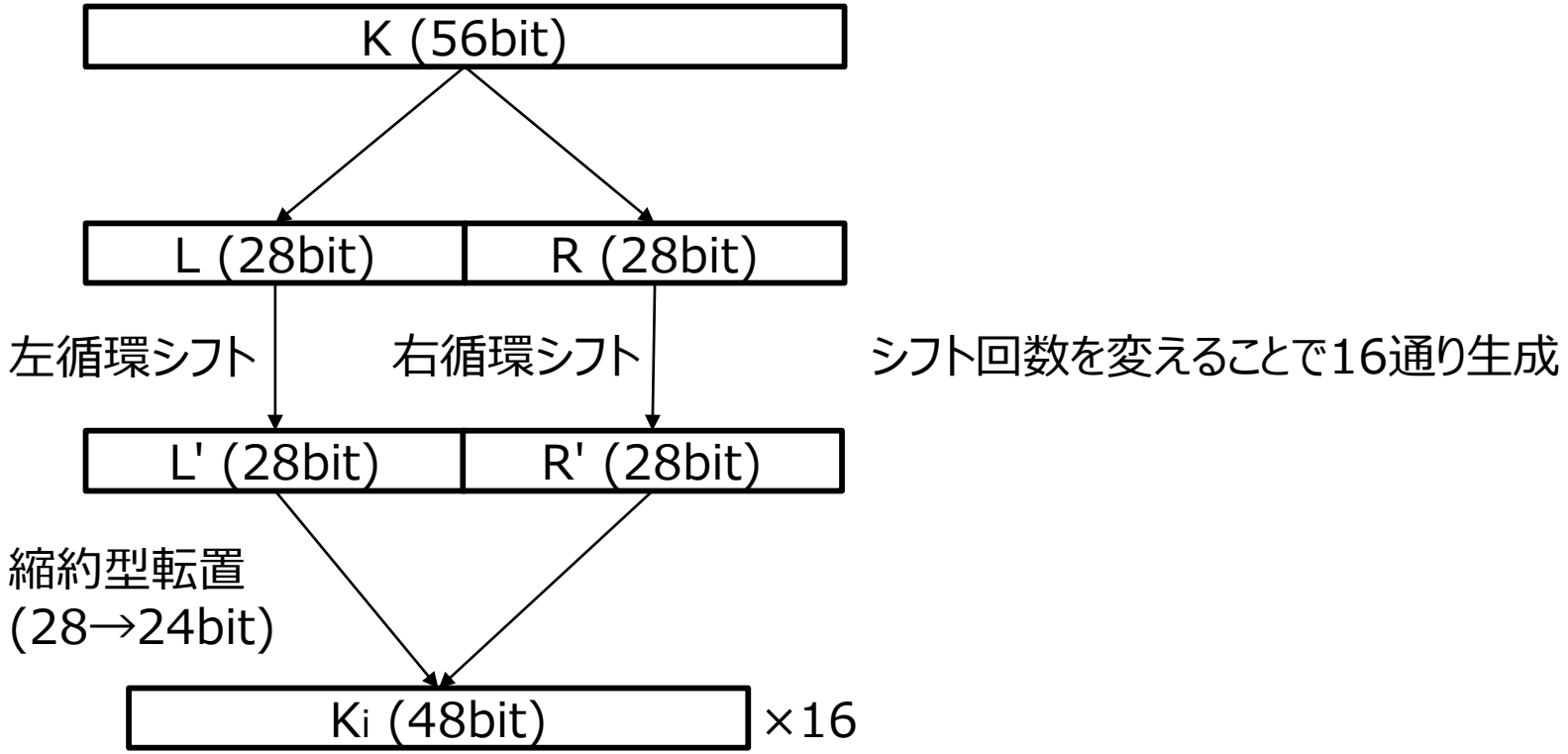
DESアルゴリズム(全体)



各ラウンドの処理

DES

鍵の生成


K (56bit)
L (28bit)
R (28bit)
左循環シフト
右循環シフト
シフト回数を変えることで16通り生成
L' (28bit)
R' (28bit)
縮約型転置
(28→24bit)
Ki (48bit)
×16

DESの安全性

- 近年の計算機性能の向上により、
  全数探索法(総当たり攻撃)による
  解読が可能に
- 3DES：異なる鍵を使って3回DESを使用
  - 現状では十分安全とされている
  - 推奨期間2030年まで
    → より安全なAES等に置き換わっている

確認問題

- 以下の各文は正しいか。○か×で答えよ。
  - 共通鍵暗号方式では、暗号鍵は公開されることが一般的である。
  - 公開鍵暗号方式では、暗号鍵と復号鍵は同一でなければならない。
  - 平文の文字の場所をある法則に基づき交換する方式の暗号を換字式暗号と呼ぶ。
  - DESでは、暗号化と復号の際、それぞれ異なる鍵を使用する。

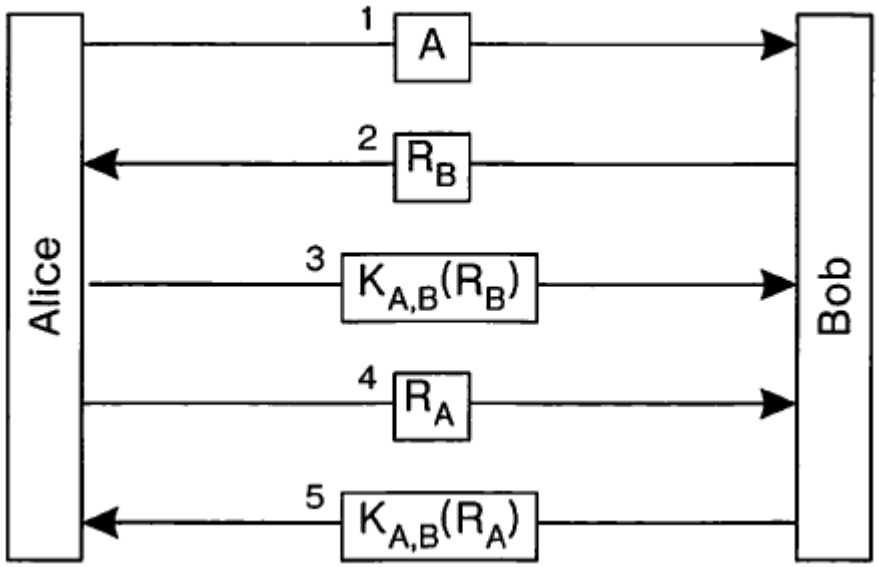
講義内容

- セキュリティ
  - 概説
    - セキュリティ特性、脅威、ポリシー
  - 暗号
  - 認証
  - 署名

認証

- 認証：適切なユーザであることを保証すること
- 送信元・送信先の正当性(＝認証) と
  メッセージの完全性(＝署名) 両方が必要
  - AがBにmを送るとき、
    送信元は確かにAか？
    送信先は確かにBか？
    メッセージは本当にmか？

共有秘密鍵に基づく認証



あらかじめ鍵$K_{A,B}$ を共有

AはBに身元識別子を送る

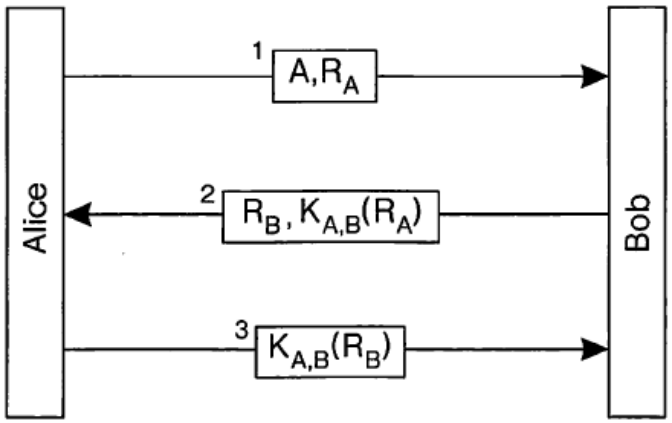
BはAに応答する(チャレンジ)

共有鍵$K_{A,B}$で暗号化したR_Bを送る
Bは$K_{A,B}$により復号できる
(Bは相手が確かにAだと確認)

Aも相手が確かにBだと確認

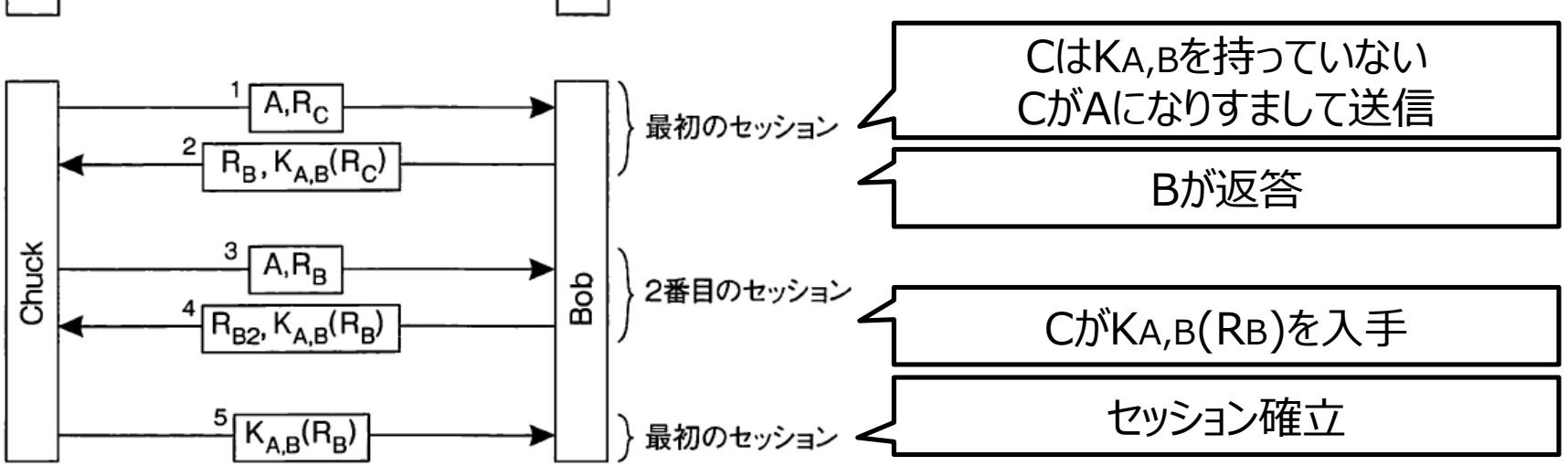
※チャレンジ：相手に応答を請求。乱数が使える

共有秘密鍵に基づく認証



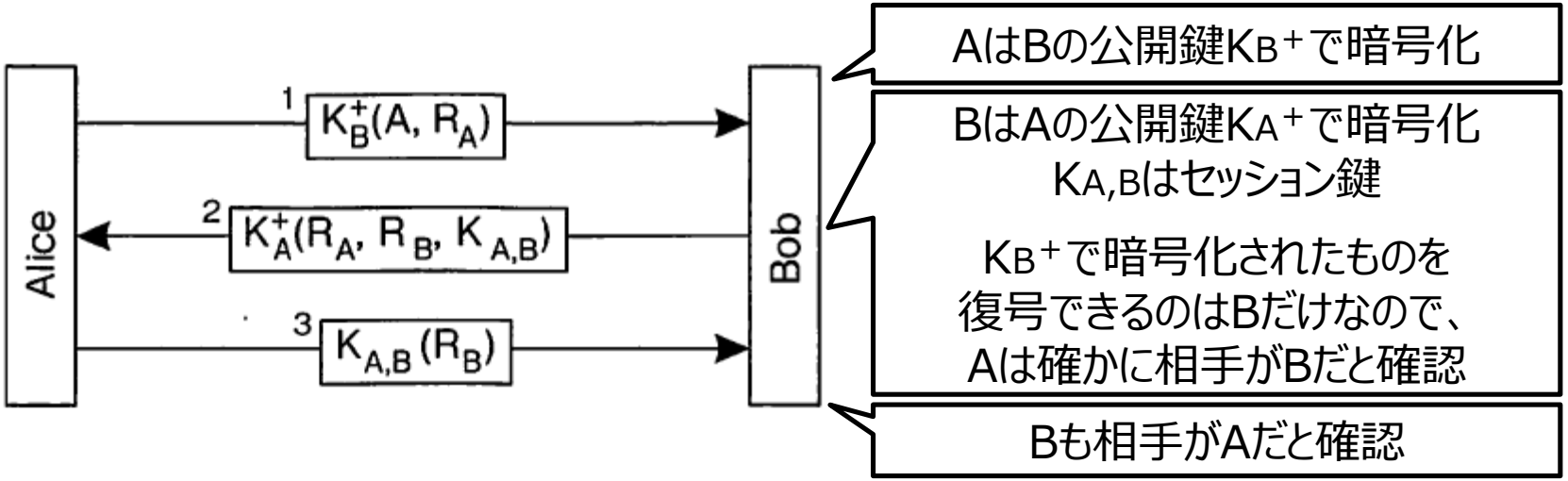
認証は容易に破られる

← このように簡略化すると…



リフレクション攻撃 (reflection attack)

公開鍵に基づく認証



- あらかじめ鍵を共有する必要がない
- リフレクション攻撃の心配もない

講義内容

- セキュリティ
  - 概説
    - セキュリティ特性、脅威、ポリシー
  - 暗号
  - 認証
  - 署名

メッセージの機密性・完全性

(再掲)

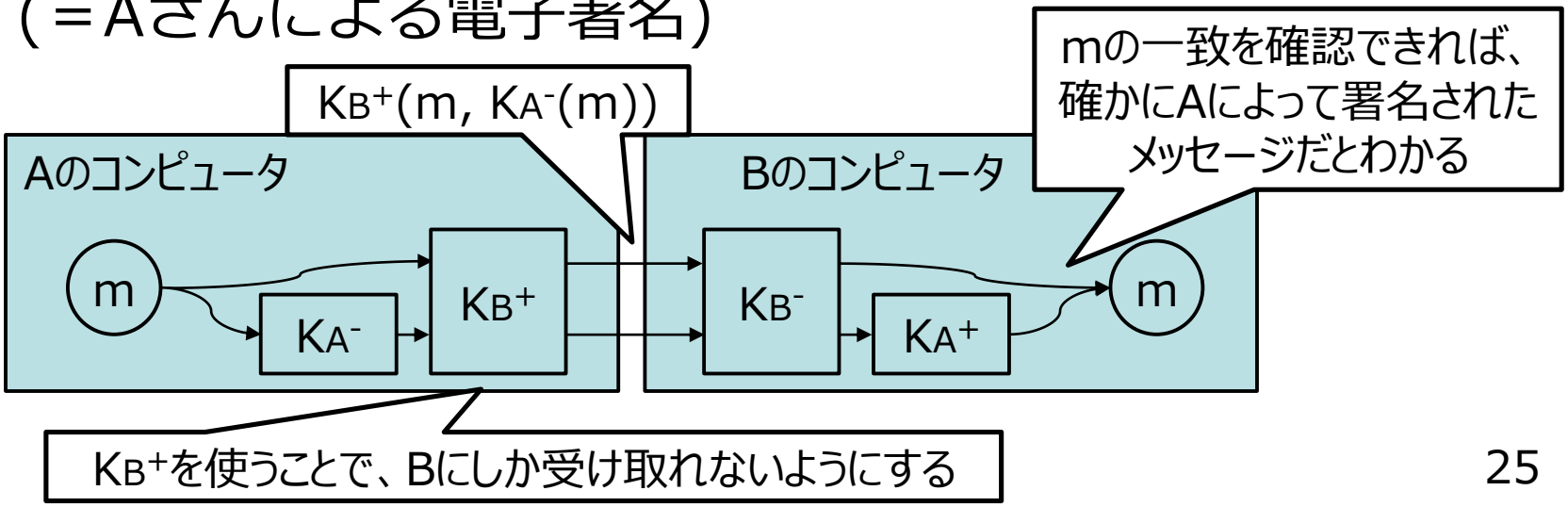
- 機密性(Confidentiality)
  - システムが情報を認可されたユーザに対してのみ開示する
- 完全性(Integrity)
  - システムの資産への改変が認可された方法でのみ行われる
    → 不当な改変は検知・修正する必要がある

- 暗号化すれば機密性は保たれる
- しかし、暗号化したものを改竄される可能性はある

- 電子署名
  - 断りなく内容を変更することを防止

公開鍵暗号による電子署名

- 通常は公開鍵を暗号化に使用
  (秘密鍵を復号に使用)
- 秘密鍵を暗号化に使用
  (公開鍵を復号に使用)すると…
  → 誰でも受け取れるが、Aさんの秘密鍵を
  持っている人物はAさんのみであるため、
  Aさんからの情報だと保証できる
  (＝Aさんによる電子署名)

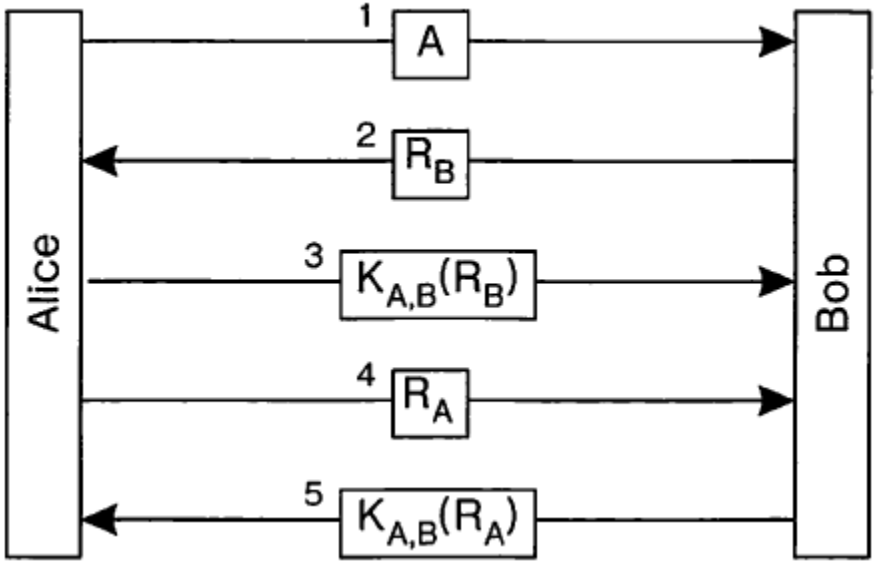


確認問題

- 以下の各文は正しいか。○か×で答えよ。
  - 認証により、送信元や送信先が適切なユーザであることを保証することが可能である。
  - 送信元と送信先が適切に認証されていれば、それらの間の通信は安全である。
  - 公開鍵暗号による電子署名では、通常、自分の公開鍵を暗号化に使用する。

確認問題

- 以下の文は正しいか。○か×で答えよ。
  - 下図において、メッセージ3とメッセージ4を連結して$K_{A,B}(R_B,R_A)$としても安全である。



参考文献

- 「分散システム」
  水野 忠則 監修、共立出版、2015
- 「分散システム 原理とパラダイム 第2版」
  アンドリュー・S・タネンバウム 他 著、
  ピアソン・エデュケーション、2009
- 「暗号の世代交代」、山岸 篤弘、
  https://www.ipa.go.jp/files/000013413.pdf