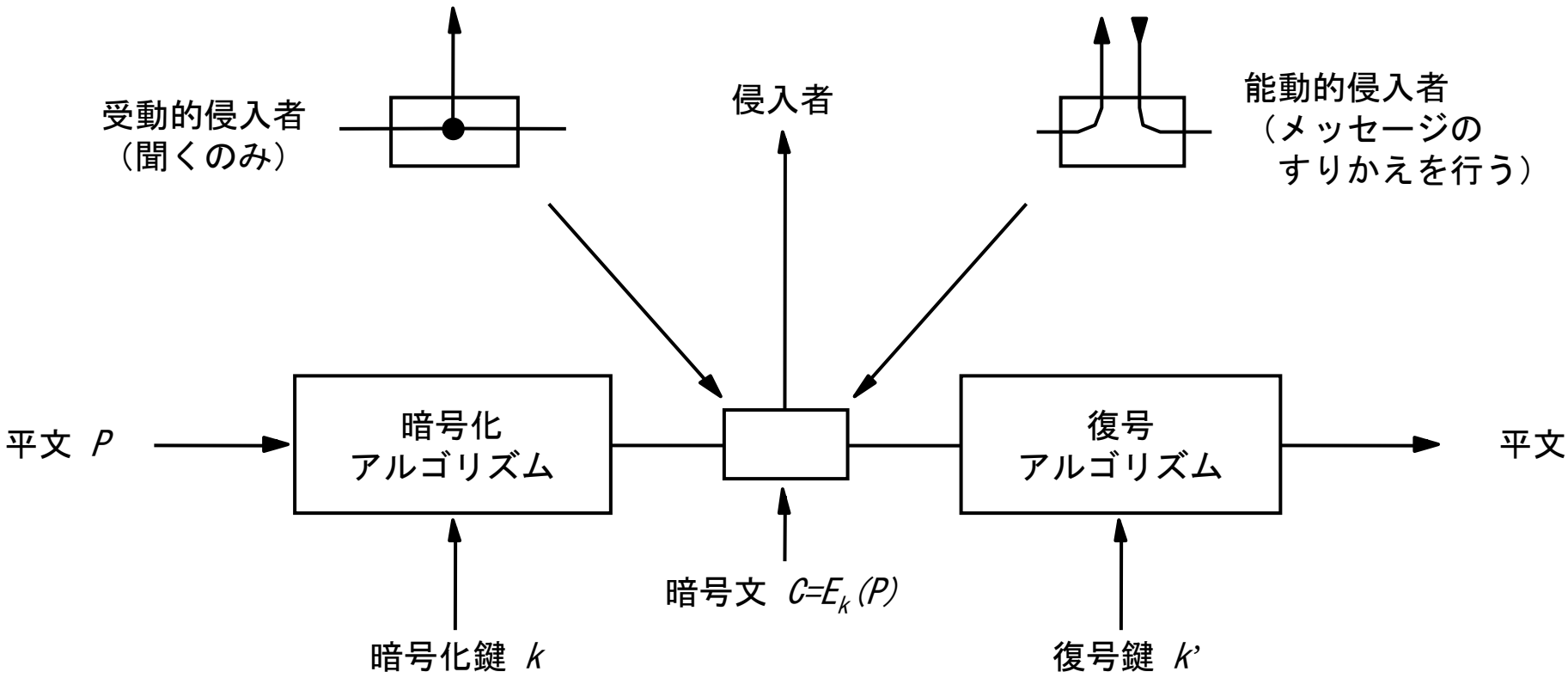
防御手段（続き）

- 暗号化
- 認証
  - パスワード（ワンタイム・チャレンジレスポンス）
  - ICカード
  - バイオメトリクス
- デジタル署名

4.2 暗号技術

暗号のモデル


受動的侵入者
（聞くのみ）
侵入者
能動的侵入者
（メッセージの
すりかえを行う）
平文 P
暗号化
アルゴリズム
復号
アルゴリズム
平文
暗号文 C=E_k (P)
暗号化鍵 k
復号鍵 k'

暗号解読のレベル

- 暗号文のみ
- 既知平文
  - いくつかの暗号文と対応する平文が与えられている（例：PLEASE LOGIN）
- 結託攻撃
- 選択平文
  - 暗号化すべき平文を解読者が指定できる

暗号方式の分類

- 共通鍵（対称鍵、秘密鍵）暗号
  - 換字式暗号
  - 転置式暗号
  - プロダクト暗号
- 公開鍵（非対称鍵）暗号

換字式暗号

- 例：単一アルファベット換字
  - a→Q, b→W, c→E, d→R, e→T, f→Y, …
  - 26!通りの鍵があり得る
- 統計的性質を用いると容易に解読可能
  - 例：文字の出現頻度 e, t, o, a, n, i, …
    th, in, er, re, an, …
    the, ing, and, ion, ...

転置式暗号

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

平文

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

暗号文

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRCXB

絶対に「解読」できない暗号

- バーナム暗号
  - ガイガーカウンタで採取するなどした真の乱数を鍵として平文と排他的論理和をとる
  - 鍵は使い捨てにする

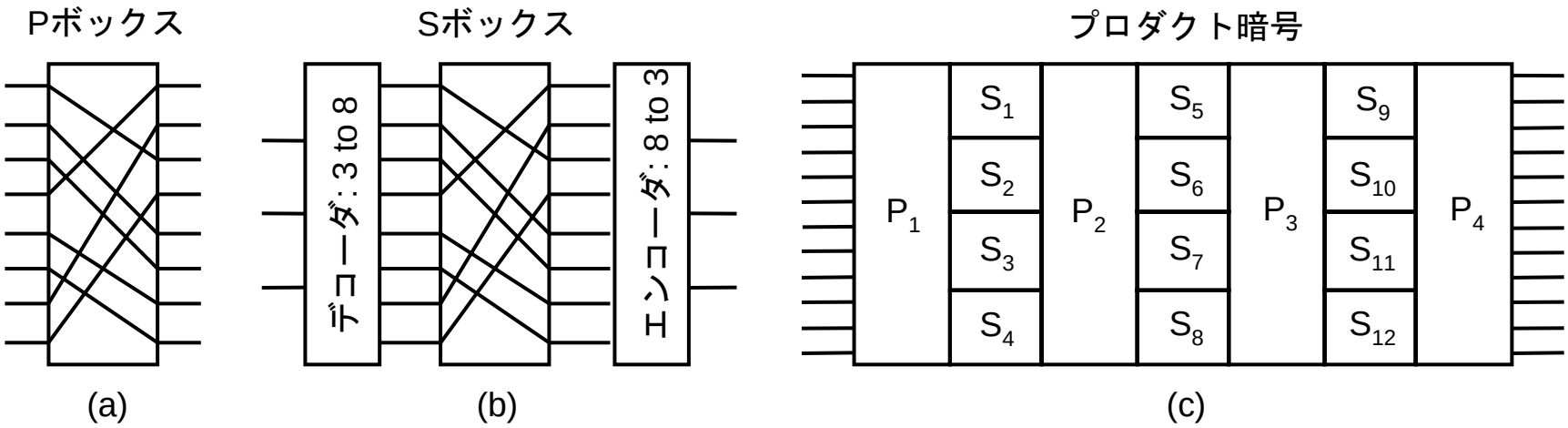
  - 送信する総データ量より長い鍵が必要
  - 鍵を送受信者で安全に共有する必要

→実用にはならない

教訓

- 暗号のアルゴリズムには平文と暗号文の対応関係がわからない程度の複雑性を持たせ、個々の通信文の秘密は鍵を頻繁に変えることで維持
- 暗号のアルゴリズムは公開し、脆弱性がないか皆で検討

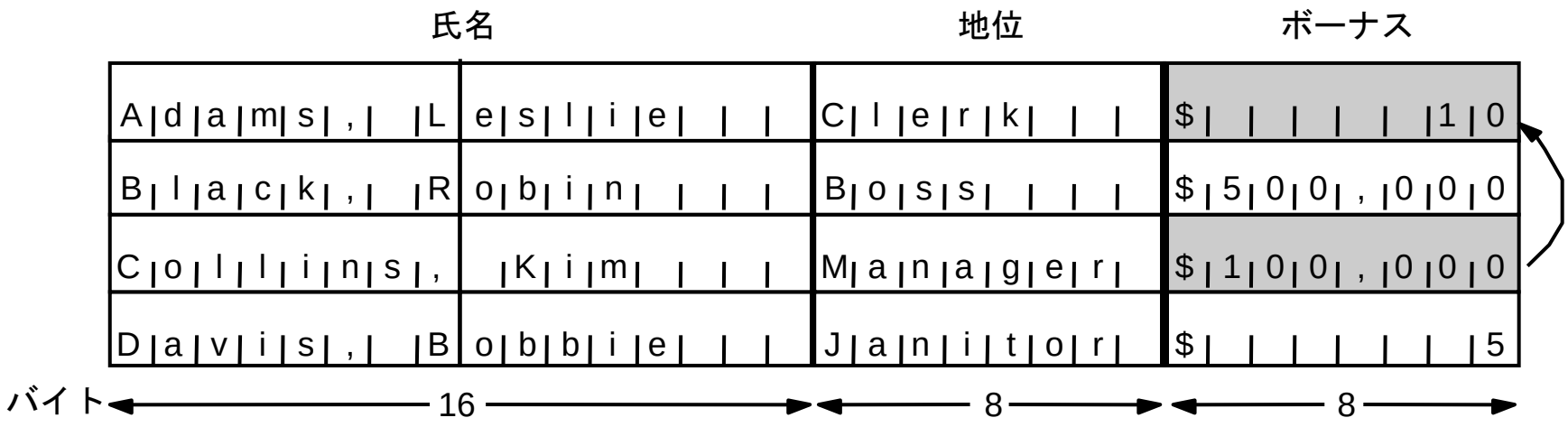
プロダクト暗号


Pボックス
Sボックス
プロダクト暗号
デコーダ: 3 to 8
エンコーダ: 8 to 3
P1
P2
P3
P4
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
(a)
(b)
(c)

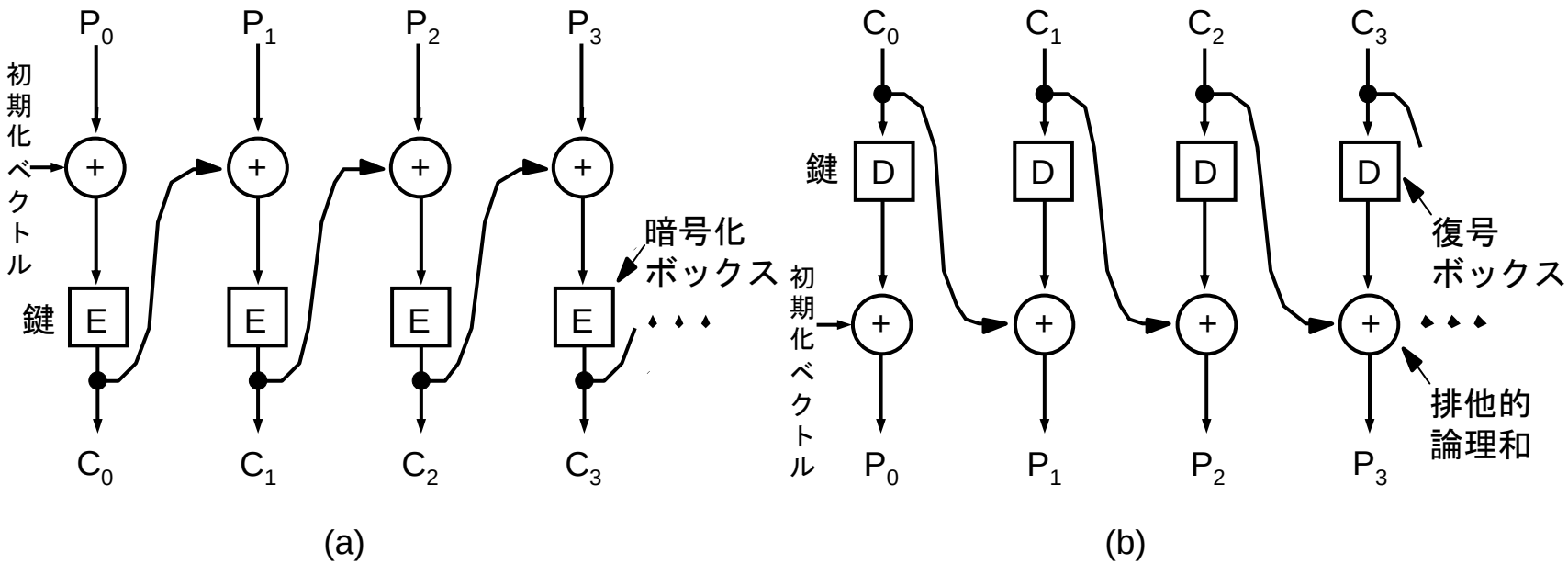
標準暗号方式

- DES (Data Encryption Standard)
  - 64ビットブロック
  - 56ビット鍵
- IDEA (International Data Encryption Algorithm)
  - 64ビットブロック
  - 128ビット鍵
- AES (Advanced Encryption Standard)
  - 128ビットブロック
  - 128ビットまたは256ビット鍵

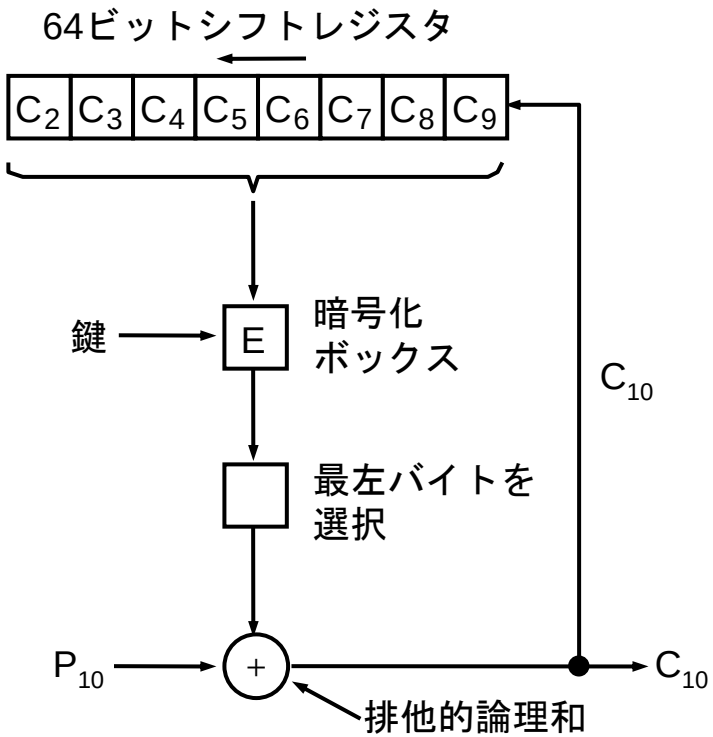
電子符号ブックモードの問題点



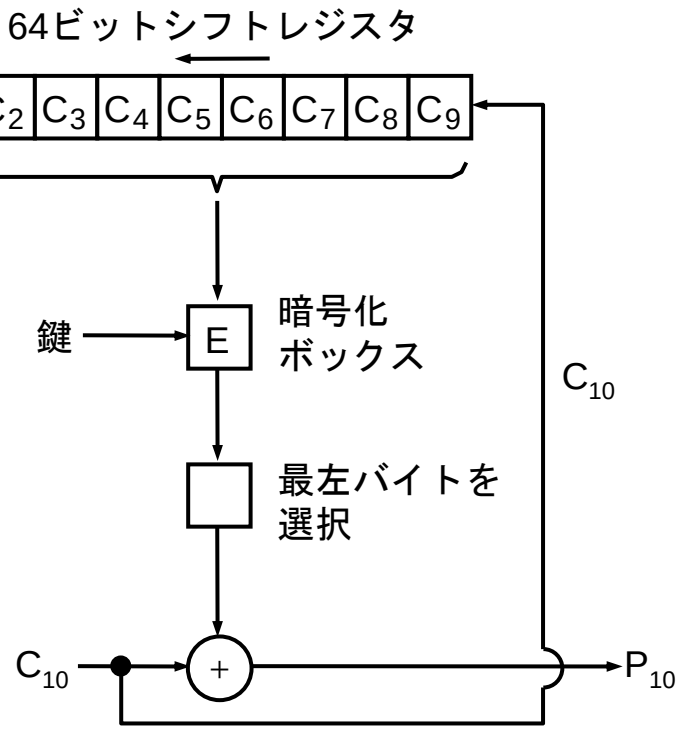
暗号ブロック連鎖方式


P0
P1
P2
P3
初期化ベクトル
鍵
E
暗号化ボックス
C0
C1
C2
C3
(a)
C0
C1
C2
C3
鍵
D
復号ボックス
初期化ベクトル
排他的論理和
P0
P1
P2
P3
(b)

暗号フィードバックモード



(a)



(b)

公開鍵暗号

- $D_{k'}(E_k(P))=P$
- E_kから$D_{k'}$を推測することはきわめて難しい（選択平文攻撃によっても$D_{k'}$は破られない）
  - 例：大きな数の因数分解、離散対数、楕円曲線上の整数座標点

→E_kは公開してよい

RSA暗号

- 鍵の準備
  - 大きな2つの素数pとqを選ぶ（$>10^{100}$）
  - $n=p\times q$と$z=(p-1)\times(q-1)$を計算
  - zと互いに素な数eを見つける
  - $(e\times d) \bmod z=1$を満たすdを見つける
- 暗号化：$E_{e,n}(P)=P^e \bmod n$
- 復号：$D_{d,n}(C)=C^d \bmod n$

RSA暗号の計算例

- $p=293$, $q=347 \rightarrow n=101671$, $z=101032$
- 101032と互いに素な数 $e=285$
- $(285 \times d) \bmod 101032=1$ より $d=709$

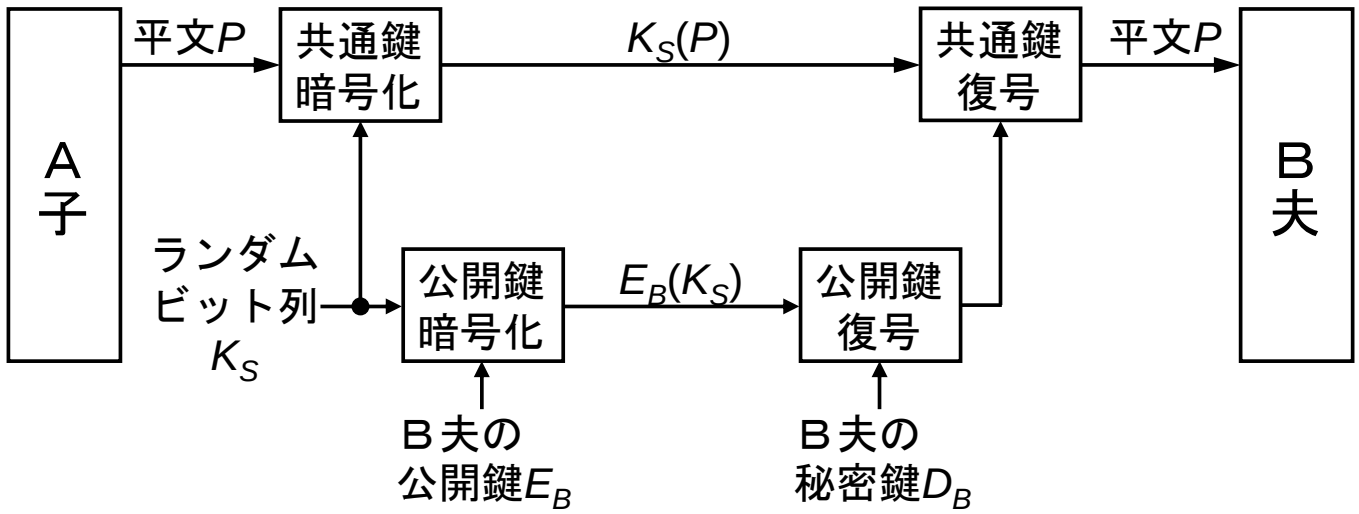
- $P=54321 \rightarrow C=P^{285} \bmod 101671=64858$
- $64858^{709} \bmod 101671=54321$

共通鍵暗号と公開鍵暗号の比較

- 共通鍵暗号
  - 必要な鍵の総数：$n(n-1)/2$
  - 各ユーザは$(n-1)$個の鍵を安全に保持する必要あり
  - 比較的高速
  - 任意のビットパタンを鍵として使用可能
- 公開鍵暗号
  - 必要な鍵の総数：$2n$
  - 各ユーザは自分の秘密鍵を安全に保持すればよい
  - 低速
  - 鍵として使用可能なビットパタンに制限有り

ハイブリッド型暗号

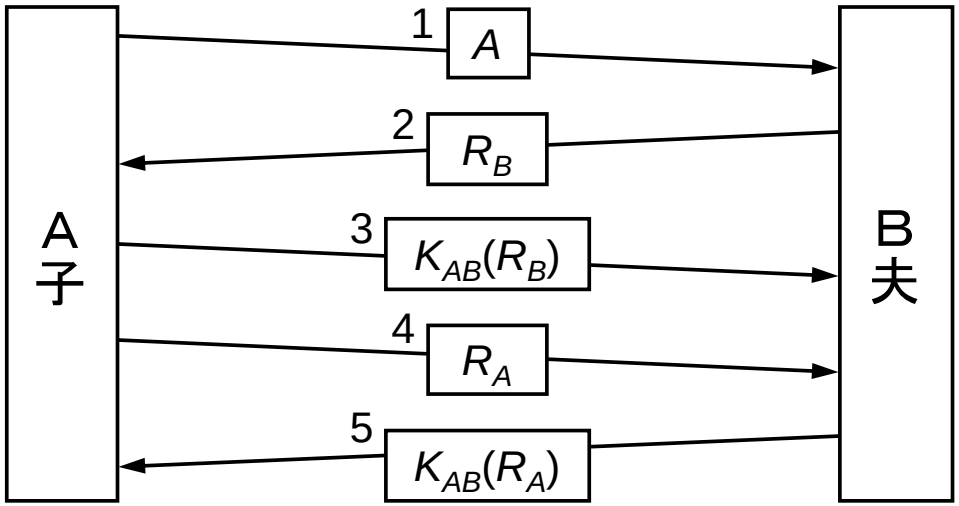
- ランダムなビット列を生成して公開鍵暗号で送り、それを共通鍵暗号の鍵として使用



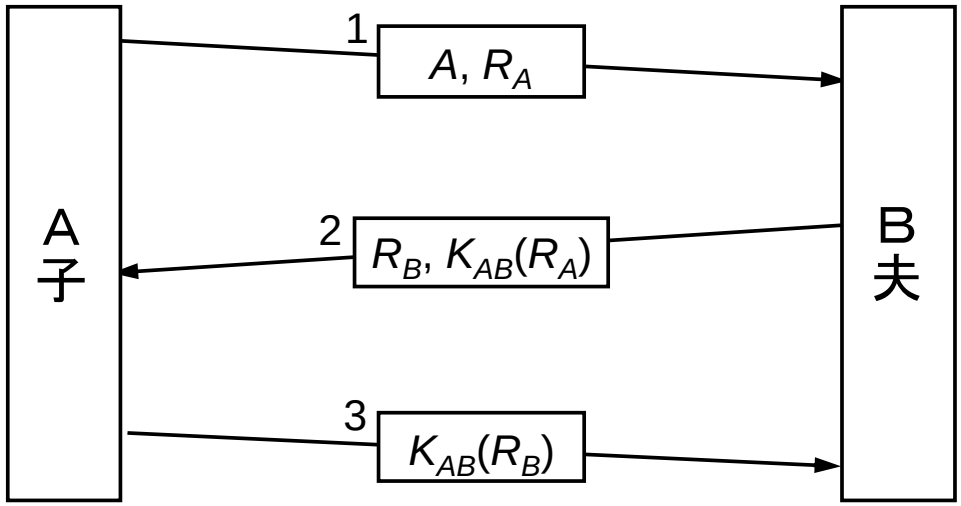
認証

- 毎回同じパスワードを用るのは危険

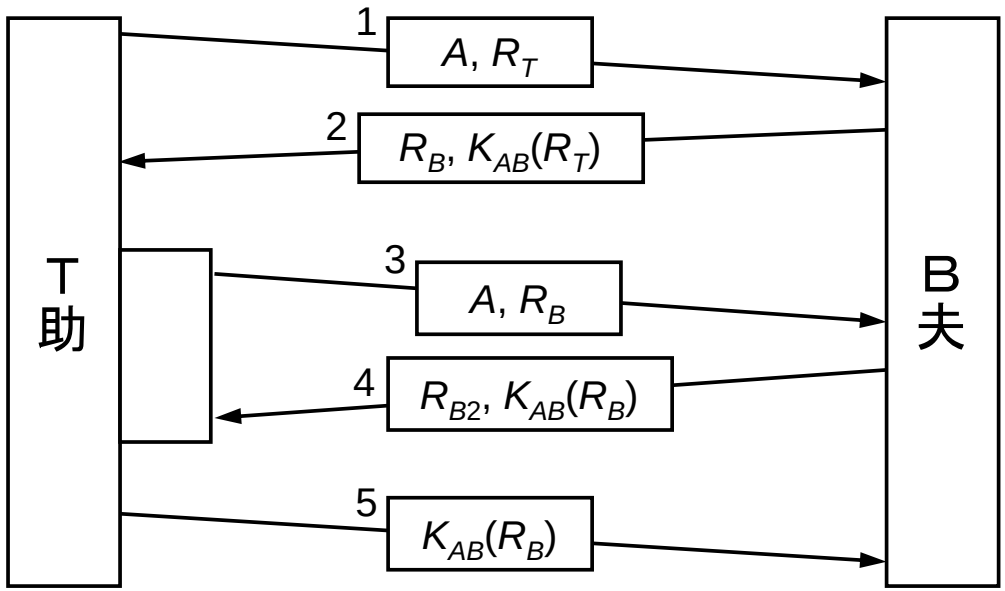
→チャレンジ・レスポンスプロトコル



プロトコルの短縮化



反射攻撃



公開鍵を用いた認証