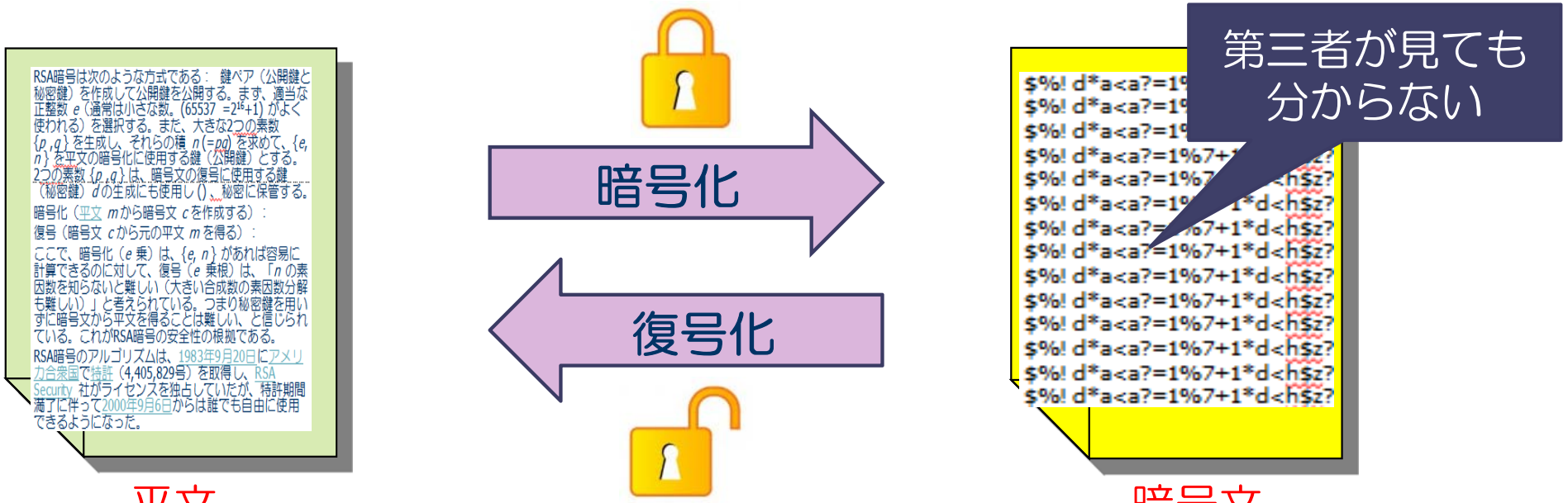
π -computerへのログイン準備

― 公開鍵と秘密鍵を作る ―

（共通鍵暗号方式と公開鍵暗号方式）

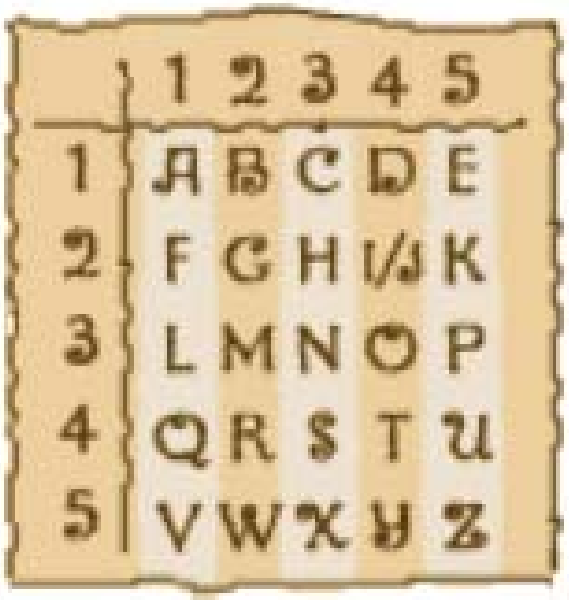
暗号とは

- 当事者以外には秘密にしておきたい情報を送るときに使う方法
- 当事者だけが，平文に鍵をかける方法，暗号文の鍵を解く方法を知っている（はず）．
- 暗号の歴史：暗号開発者と暗号解読者の知恵比べの歴史



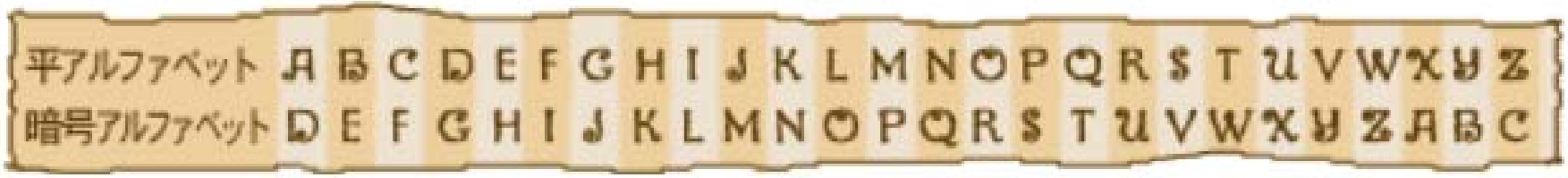
古代の暗号

- ポリュビオアスの暗号（Polybius square）
  - 紀元前2世紀
  - 文字を数字に変換
  - 1つのアルファベットを2つの数字で表す.



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- シーザー暗号（換字式暗号方式）
  - 紀元前1世紀

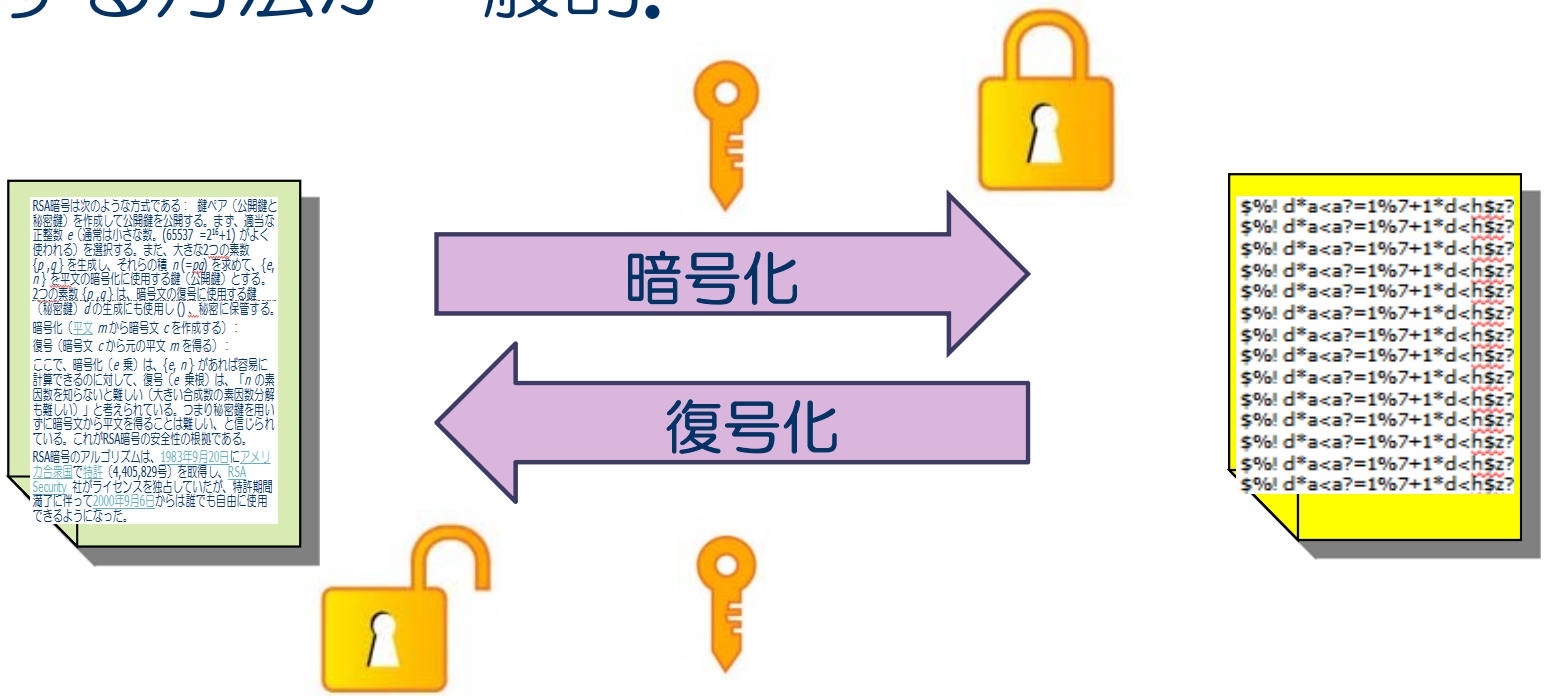


平アルファベット	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
暗号アルファベット	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

  - アルファベットを，ある数だけずらして暗号化
    - 図では左に3個ずらしている.
  - 文書に現れる文字の頻度解析により推定可能.

暗号のポイント

- 暗号文をやり取りするには，暗号化及び復号化のための暗号アルゴリズムと鍵を，双方で共有化する必要がある．
- 現代の暗号では鍵を秘密にし，暗号アルゴリズムを公開する方法が一般的．

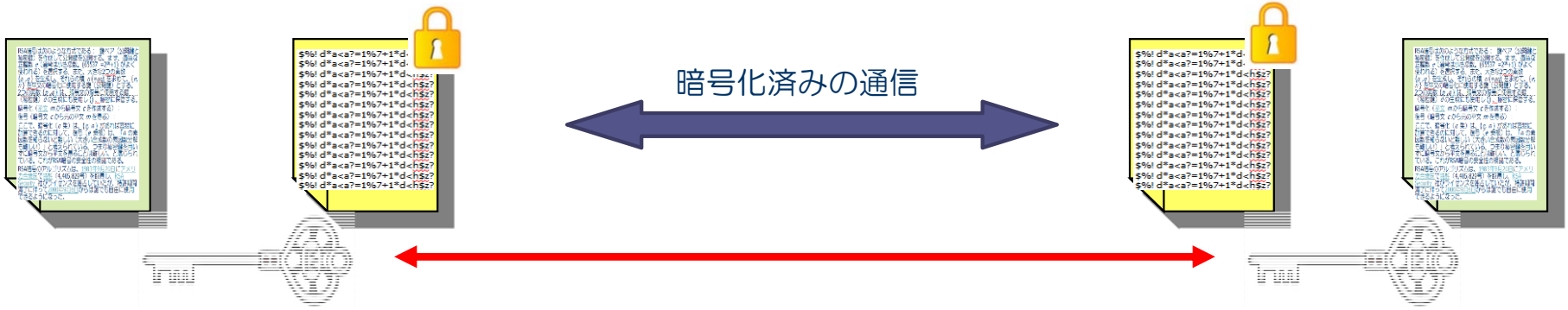


共通鍵暗号方式

- DES（Data Encryption Standard）暗号
  - 1973年 米国商務省標準局（NBS，現在のNIST: National Institute of Standards and Technology）が，米国政府が標準利用する暗号方式を募集.
  - 暗号アルゴリズムを公開（歴史上の大きな転換点）
    - 文字置換と鍵との排他的論理和などで構成.
  - 1976年 DES暗号を承認．世界的な標準暗号.
    - 民間利用においては，顧客ごとの暗号管理をする必要がなくなった.
  - 鍵
    - 64ビットのうち8ビット毎に奇数パリティ ⇒実質56ビット
    - 暗号化，復号化に用いる鍵は一つ（共通鍵暗号）.
- 暗号アルゴリズムが公開されているので，鍵を2^{56}通り，試してみれば，必ず解読できる.
  - 22,393 台の Intel Pentium II 333MHz マシンで，41日で解読できた.

共通鍵暗号方式の問題点

- （共通鍵）暗号により，鍵を共有している相手と，暗号化した情報のやり取りが可能となった．
- 暗号化，復号化の計算が高速に行える．



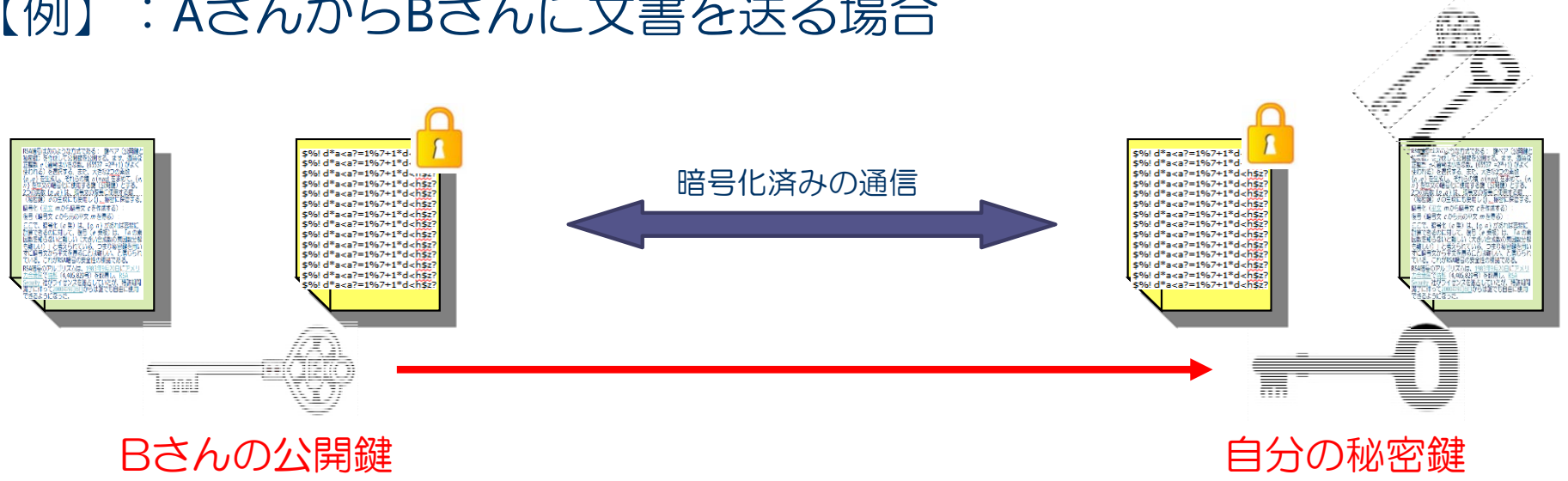
- 相手にどのように鍵を渡すか？
  - ① 暗号化しないで送る．
    ⇒ 鍵が盗聴されたら，暗号化の意味がない．
  - ② 直接会って伝える．
    ⇒ 鍵を定期的に変える場合など面倒．遠い相手には不便．
  - ③ 盗聴されないような方法（開封が分かる郵送等）で伝える．
    ⇒ 不特定多数への相手に送るのは現実的でない．

公開鍵暗号方式

- 非対称な鍵（公開鍵，秘密鍵）の２種類の鍵を使う方法．
  - 一方の鍵を公開し，もう一方は秘密にしておく．

- どちらかの鍵で暗号化した文書は，もう一方の鍵でしか復号できない．

【例】：AさんからBさんに文書を送る場合



公開鍵暗号方式：RSA暗号

- 1976年　ホイットフィールド・ディフィー，マーティン・ヘルマン，ラルフマークが，公開鍵暗号方式を発表.
  - モジュラー算術という一方向関数を用いる.
- 1977年，ロナルド・リベスト（Ronald L. Rivest），アディ・シャミア（Adi Shamir），レオナルド・エーデルマン（Leonard M. Adelman）らが発明.
  - 頭文字をつなげて，RSA暗号と呼ばれる.
  - 素因数分解を用いる方法
    - 大きな数の素因数分解はなかなか解けない.
- RSA暗号のアルゴリズムは，1983年米国特許（4,405,829号）を取得．2000年9月6日から特許期間満了に伴い自由に利用可能.
- 現実的な時間の範囲では，秘密鍵を解読することが困難.

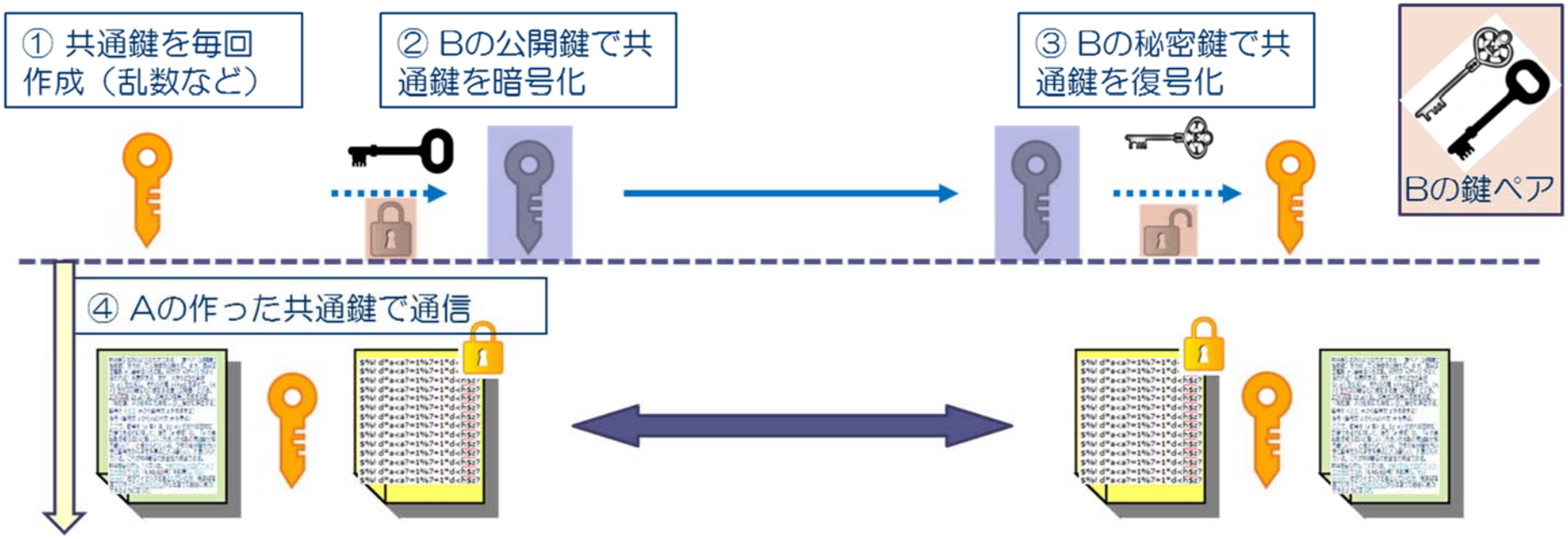
公開鍵暗号方式の利点，欠点

- 利点
  - 安全な鍵の配送を実現した．
    - 公開鍵だけ相手に送れば良い．
  - 鍵の管理の負担を軽減した．
    - 秘密に管理すべきは自分の秘密鍵だけ．

- 欠点
  - 暗号の強度を保つためには，鍵の長さを長くしなければならない．
  - 計算が複雑で，共通鍵暗号に比較して，暗号化/復号化に時間がかかる．

ハイブリッド方式

- 公開鍵暗号方式と共通鍵暗号方式を組み合わせる.



- 利点
  - 安全に共通鍵を相手に送ることが出来る.
  - 時間のかからない共通鍵暗号アルゴリズムにより，処理時間の短縮化が図れる.