暗号（3）
―公開鍵暗号―

野口　拓
Taku NOGUCHI

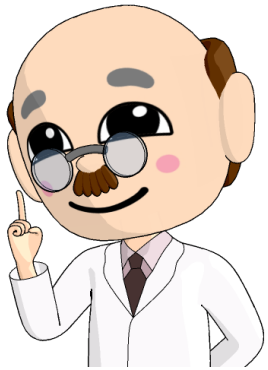
秘密鍵(共有鍵)は暗号として重要だが・・・

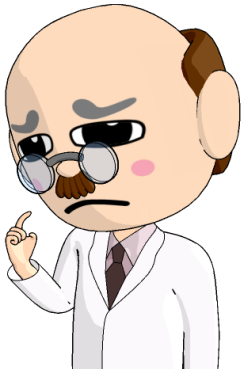
- 代表的なもの:DES, AESなど

メリット：merit

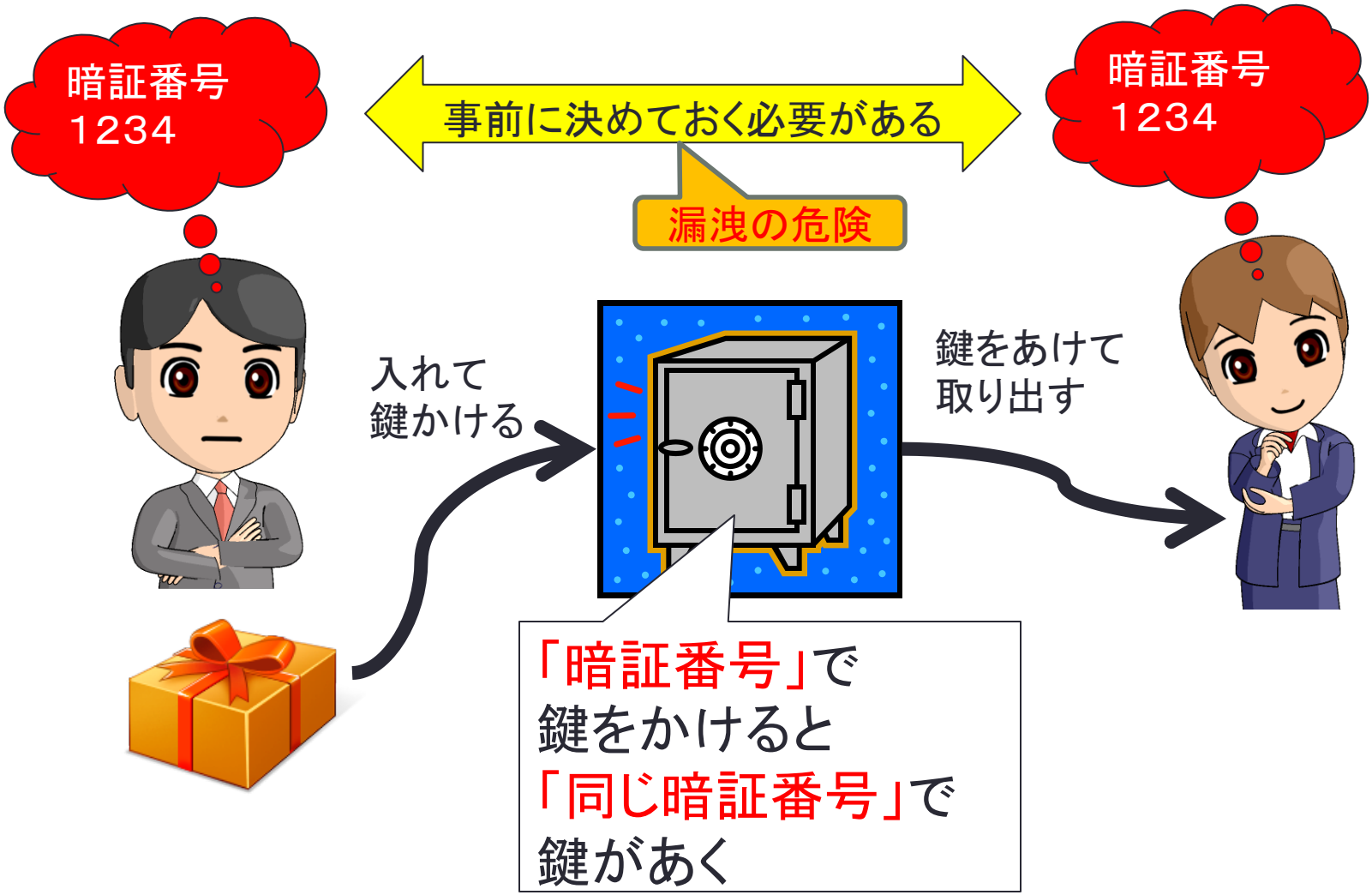
デメリット：demerit

- メリット
  - 高速かつ安全性の証明された暗号化方式(アルゴリズム)が複数知られている
  - 1対多通信・多対多間一斉通信に使える
- デメリット
  - 鍵の配送が必要で、その際に漏洩の危険がある
  - N人の人がいれば${}_{N}C_{2}$組の通信があり、鍵はその分だけ必要

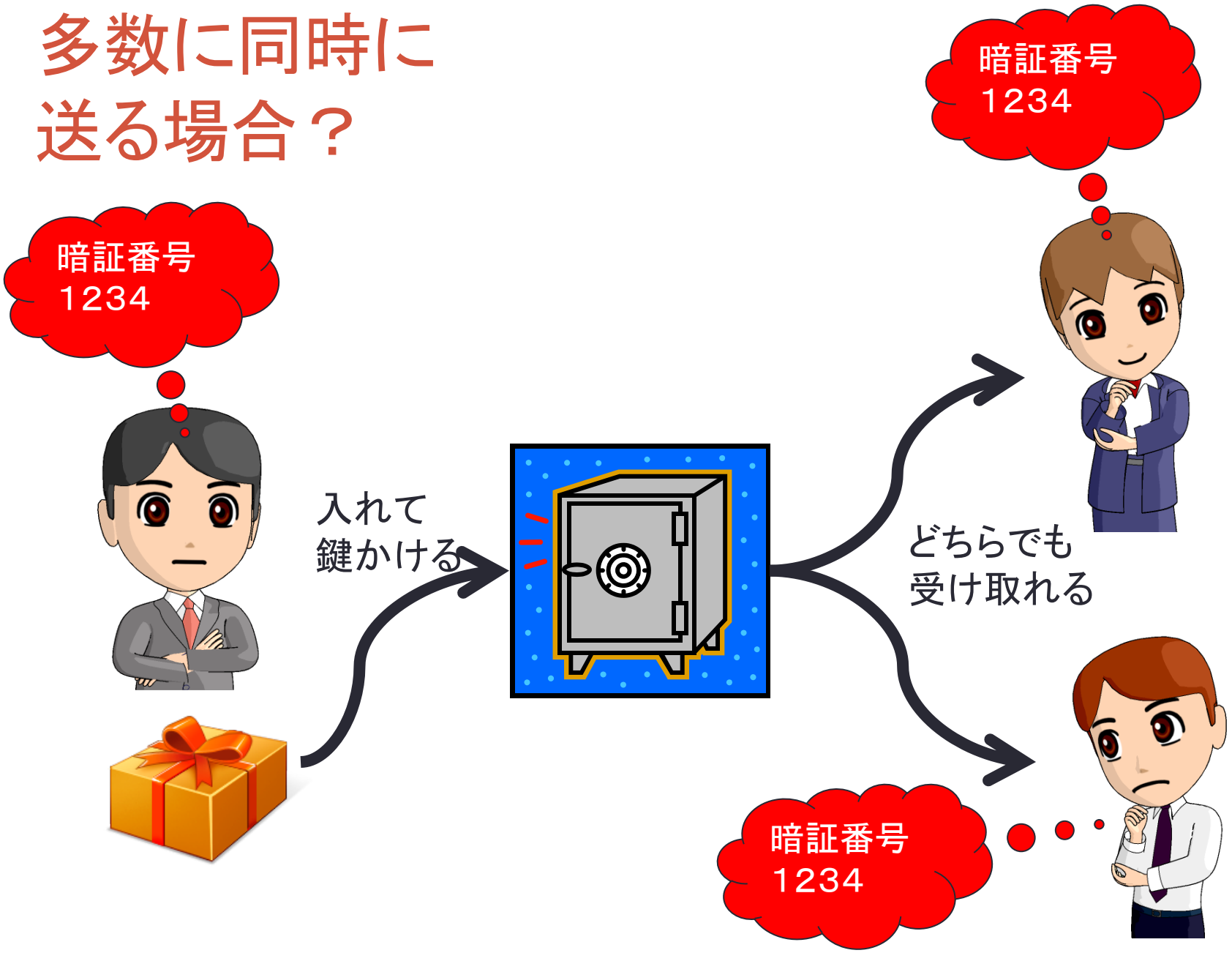




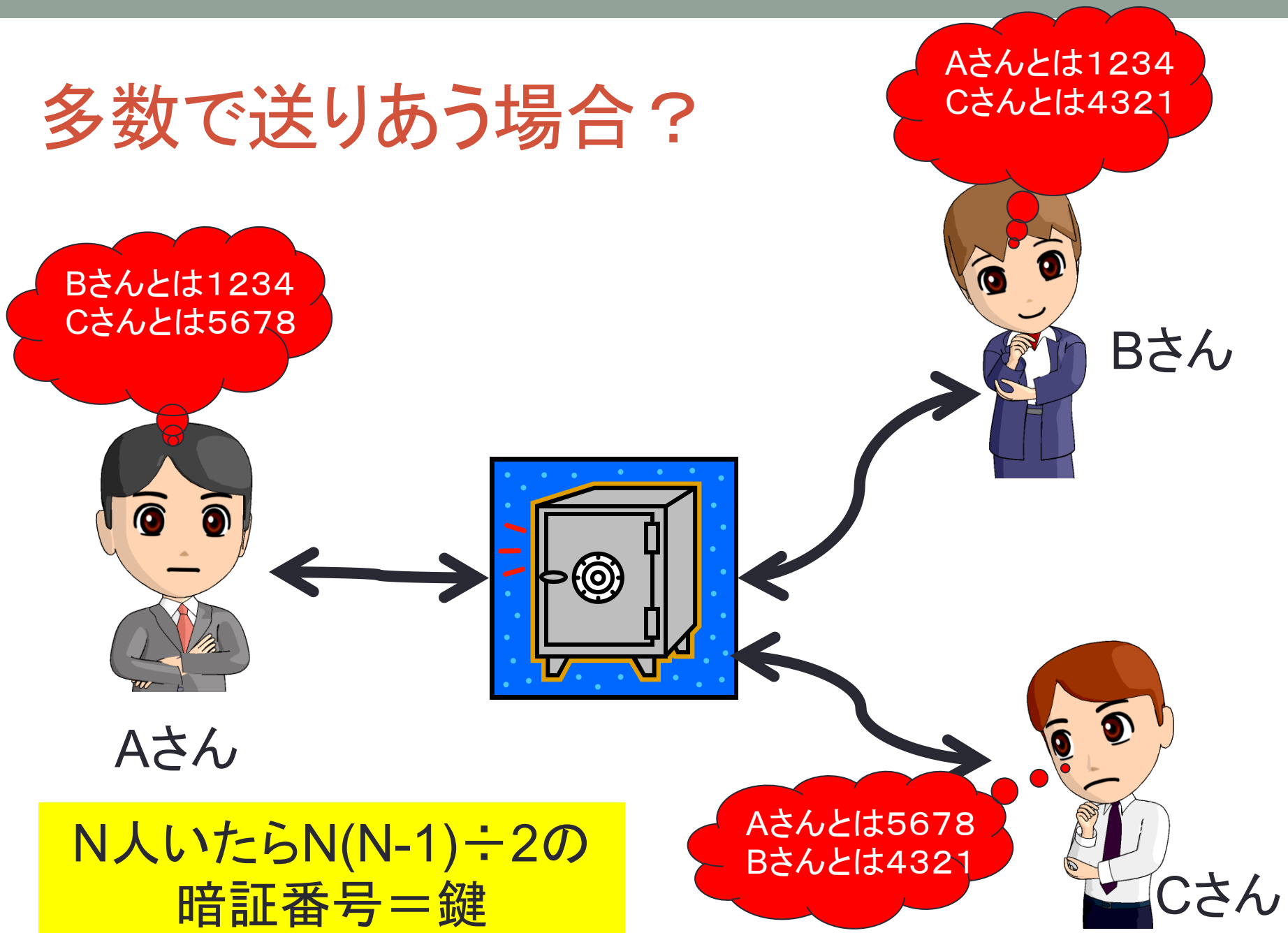
共有鍵＝暗証番号式の金庫



多数に同時に送る場合？



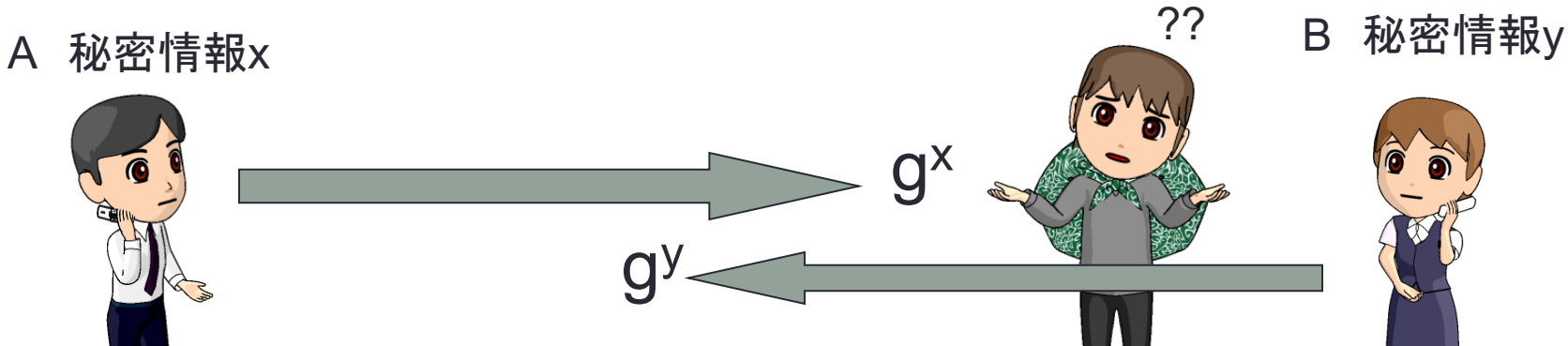
多数で送りあう場合？

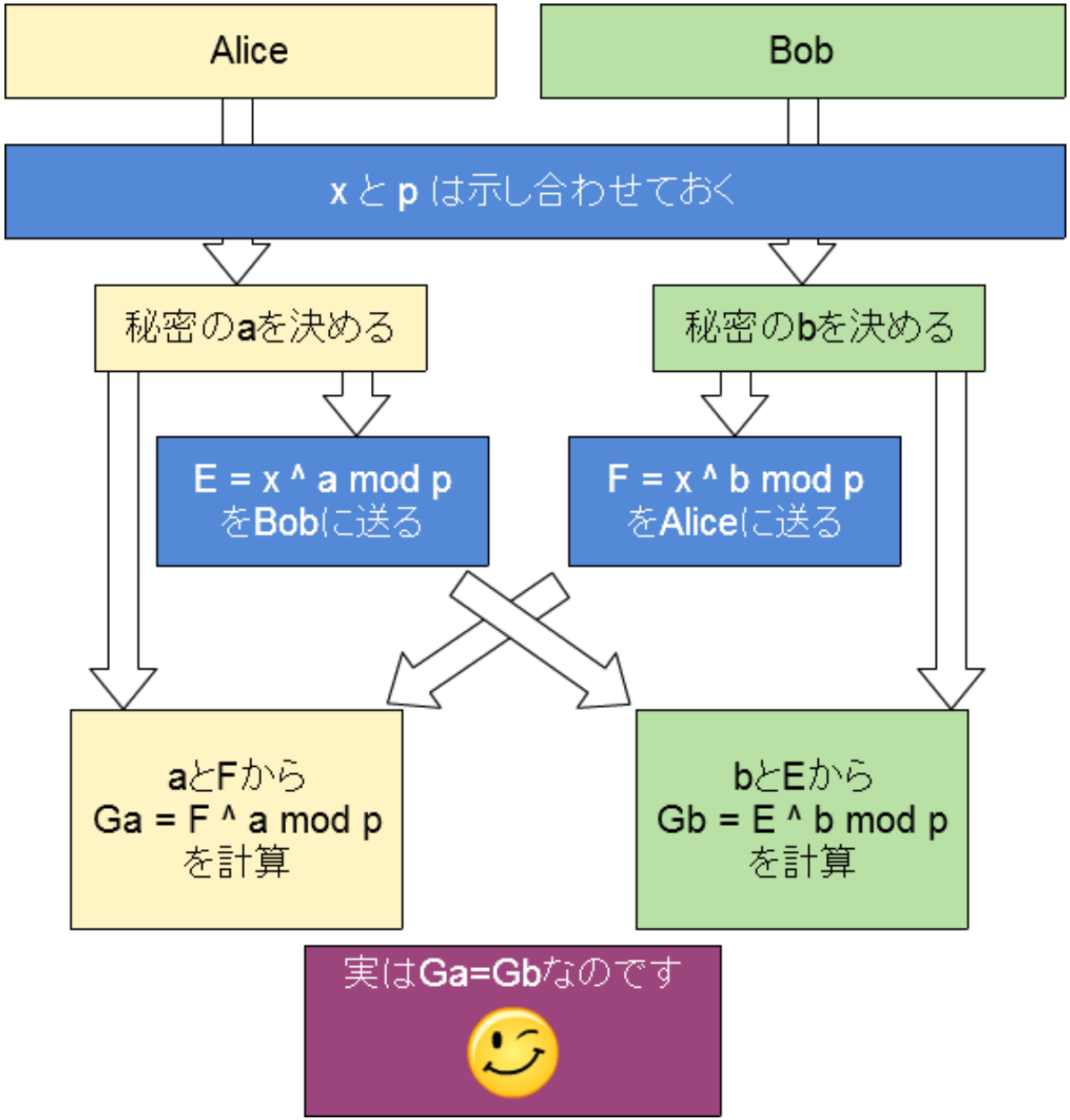


N人いたらN(N-1)÷2の
暗証番号＝鍵

鍵配送問題の解決

- 秘密共有鍵では、予め何らかの方法でお互いに鍵を共有する必要がある
- 安全に鍵を交換できる方法があればいいが、ない場合には？？
- 1976：Diffie-Hellman鍵交換 （DH鍵交換）
  - 離散対数問題（※）は困難
    （ここではa=g^x mod pを単にa=g^xと書く）
  - Aが秘密情報xを持っていて、Bが秘密情報yを持っている
  - Aはg^xを、Bはg^yをお互いに相手に送る 盗聴されてもx/yは不明
  - AとBはお互いに秘密共有鍵g^{xy}を得られる
    - g^{xy} はなんと、modしてもちゃんと$(g^x)^y$




Alice
Bob
x と p は示し合わせておく
秘密のaを決める
秘密のbを決める
E = x ^ a mod p
をBobに送る
F = x ^ b mod p
をAliceに送る
aとFから
Ga = F ^ a mod p
を計算
bとEから
Gb = E ^ b mod p
を計算
実はGa=Gbなのです

離散対数問題 (Discrete Logarithm Problem; DLP)

- 整数の集合Z、素数pについて
  - Z mod p : 整数を p で割った余りの集合
  - p=7のとき: {0,1,2,3,4,5,6}
- 0を除く全ての Z mod p の要素について、x∈Z mod p のべき乗を考える
  - p=7, x=3 のとき: $3^1=3$, $3^2=2$, $3^3=6$, $3^4=4$, $3^5=5$, $3^6=1$
- ある要素のべき乗の集合が全ての元を生成するとき、その要素を原始元という
  - 3は Z mod 7 の原始元
- 離散対数問題: a,g∈Z mod p (ただし g は原始元)について $g^i \bmod p = a$ となる整数解 i を求める問題
  - p=5, g=3, a=1 のとき、i はどうなる？
- p や g が大きくなると求めるのは難しい。この性質は暗号で広く用いられている

つまり

- $g^i \bmod p = z$ (p は大きな素数) のとき
  - (g,i,p)からzを求めるのは簡単
  - (g,z,p)からiを求めるのは難しい

たとえばp＝7としてみる

g \ x	1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	4	1	2	4	1	2	4	1	2	4	1	2
3	3	2	6	4	5	1	3	2	6	4	5	1	3
4	4	2	1	4	2	1	4	2	1	4	2	1	4
5	5	4	6	2	3	1	5	4	6	2	3	1	5
6	6	1	6	1	6	1	6	1	6	1	6	1	6

$g^x \bmod 7$

p=19, g=3

① p=19, g=3に決定！

② x=8
$3^8 \bmod 19$
$=6561 \bmod 19$
$=6$

③ 6

② y=12
$3^{12} \bmod 19$
$=531441 \bmod 19$
$=11$

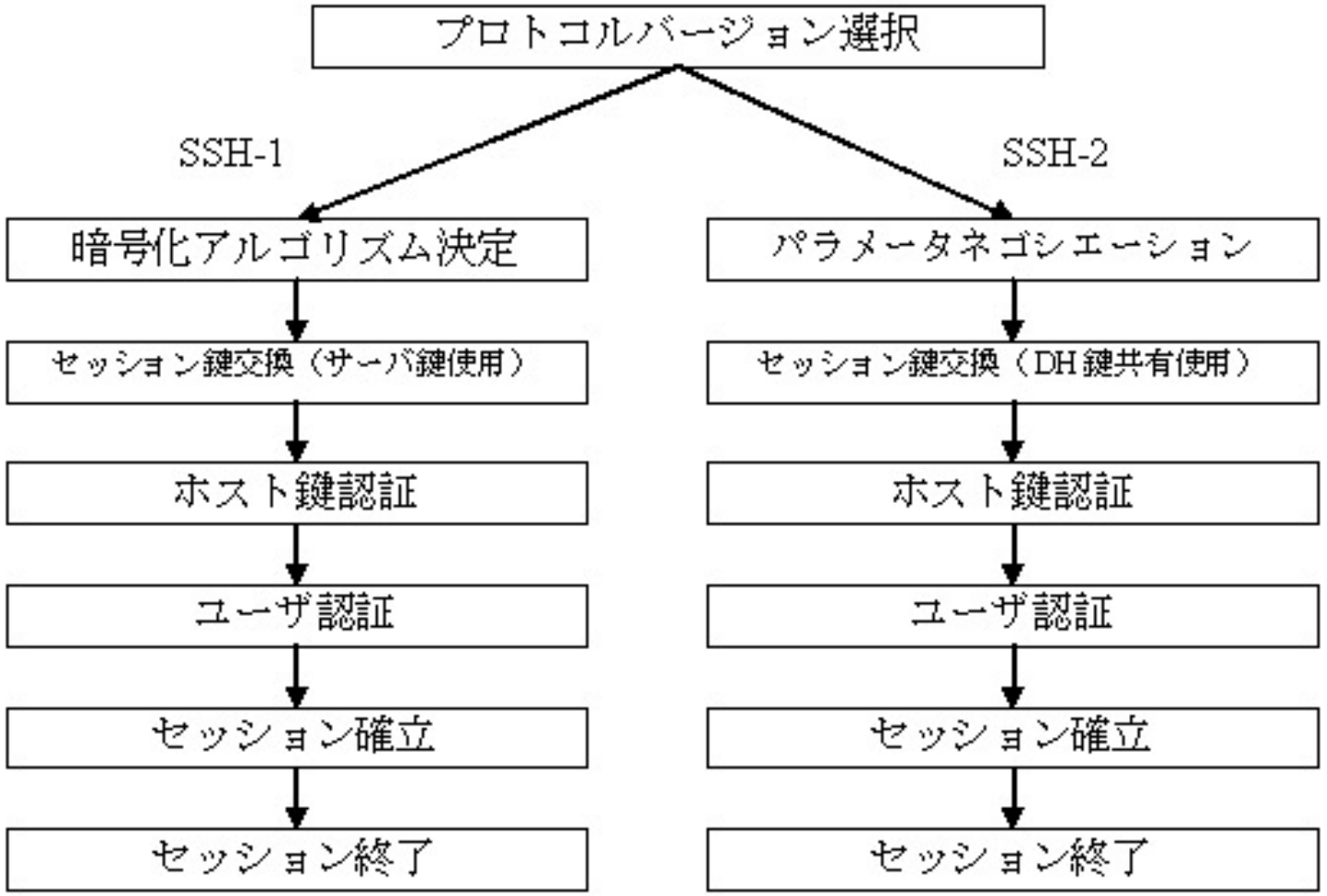
③ 11

$3^x \bmod 19=6$
$3^y \bmod 19=11$
x=?? y=???
$3^{xy} \bmod 19=???$

④ $3^y \bmod 19=11$
$3^{xy} \bmod 19$
$=11^8 \bmod 19$
$214358881 \bmod 19$
$=7$

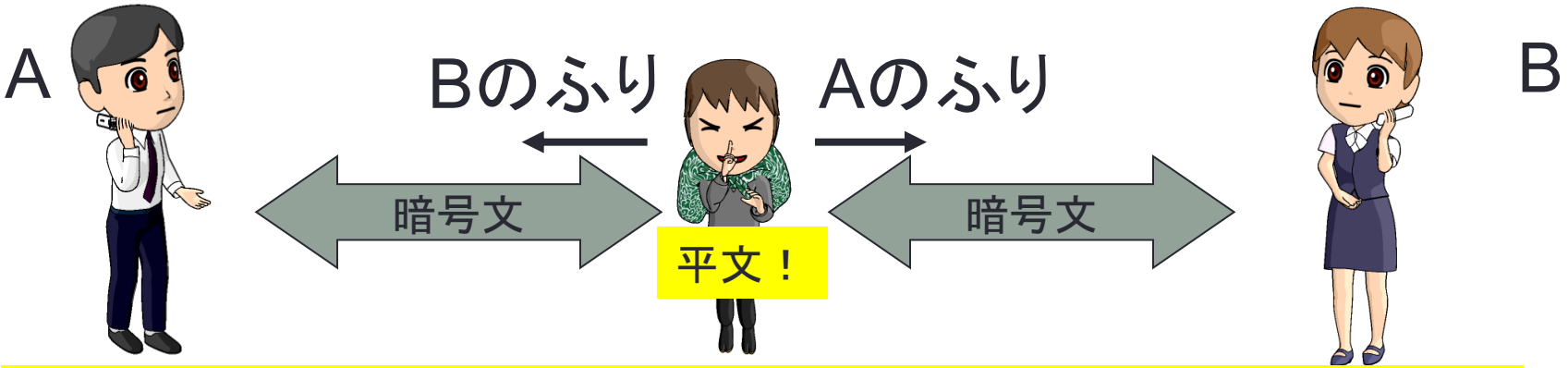
④ $3^x \bmod 19=6$
$3^{xy} \bmod 19$
$=6^{12} \bmod 19$
$2176782336 \bmod 19$
$=7$

SSHなんかでもつかわれてる



中間者攻撃

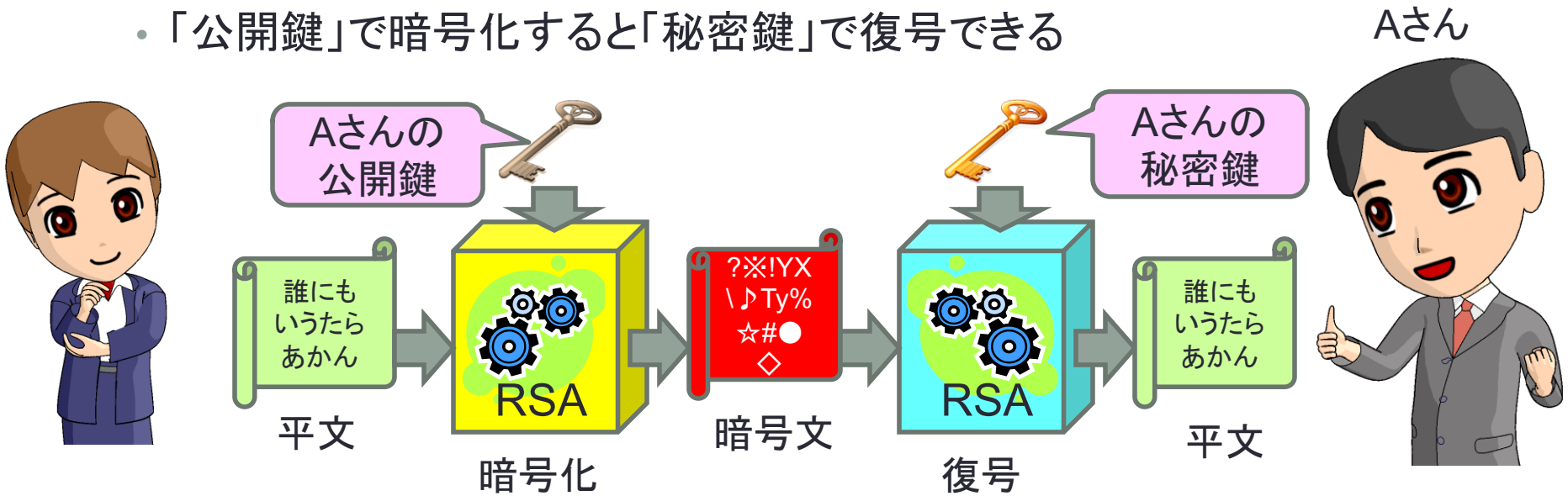
- MITM(Man-in-the-middle)攻撃ともいう
- DH鍵交換の中間に割り込むことができれば
  x,yそのものは得られずとも暗号文は解読可能
  - 通信相手の秘密情報は知ることができないので、
    本当に相手が正当な受信者か確認する手段がない



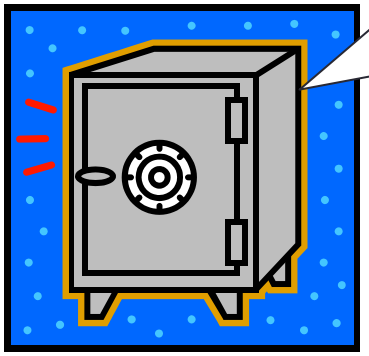
DH鍵交換で一応の解決をみた鍵配送問題が直面した難題

そこで公開鍵暗号

- DiffeとHellmanが1976年にアイデアを公表
  - 実はそれより前に英国の諜報機関で考案・開発されてたらしい
- 各人が「秘密鍵」と「公開鍵」を持つ
  - 秘密鍵は自分だけが持ち他人に教えない
    公開鍵は広く他人に教える（誰にばれてもよい）
    - 公開鍵は誰に知られてもよいので鍵配送が容易になる
      秘密鍵の秘匿は必須だが、配送の必要がないので容易
  - 「公開鍵」で暗号化すると「秘密鍵」で復号できる



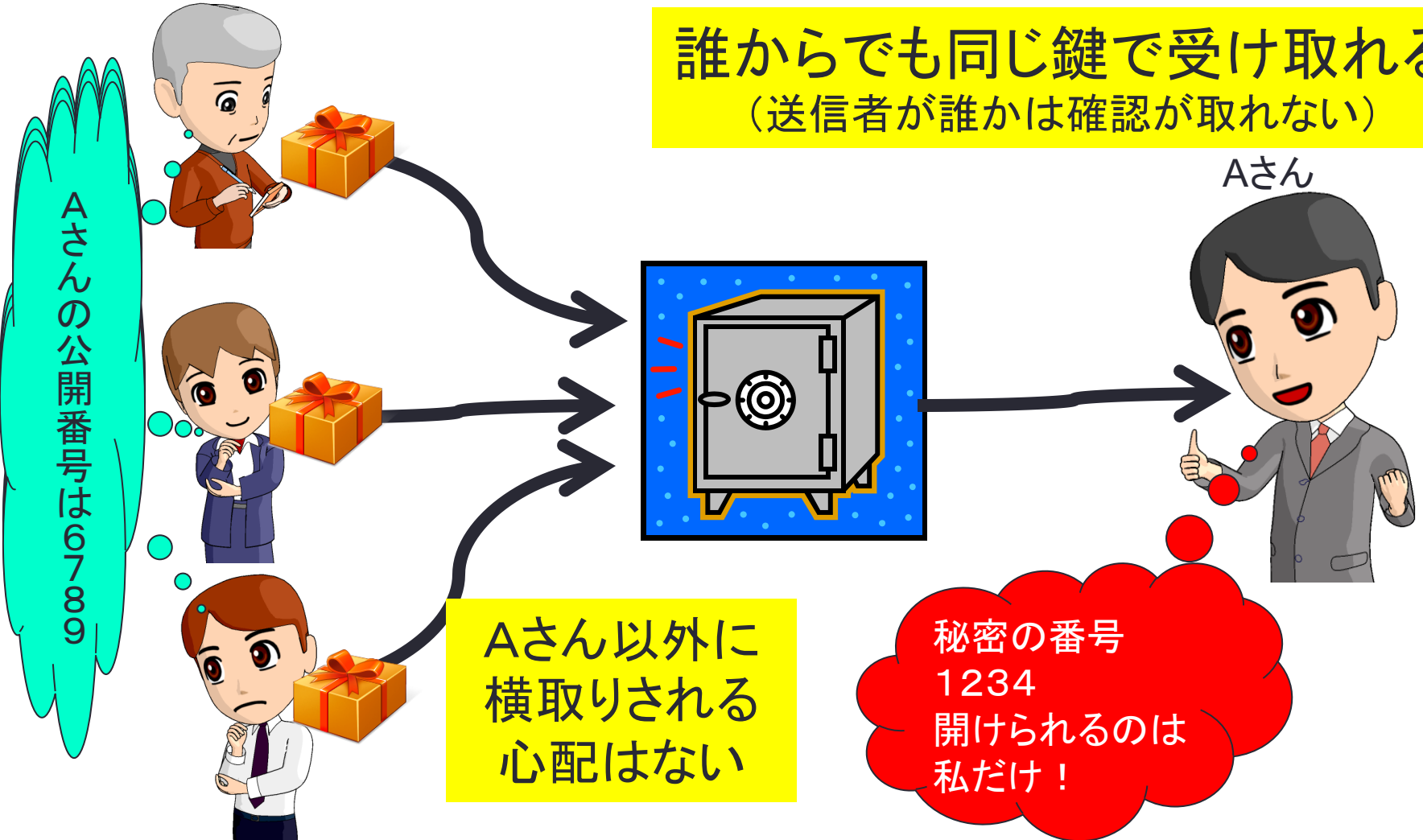
「公開鍵」
＝特殊な暗証番号式の金庫



「公開の番号」で
鍵をかけると
「秘密の番号」で
鍵があく

あらかじめ
周知
（または通信開始
直前でもよい）

Aさんに「届け物」をしたい



こんなことが可能か？
→可能だった！

- RSA暗号の発見（1978年）Rivest, Shamir, Adlemanら 実はもっと前にイギリスで。
  - 素数P、Qに対してN=PQとする
    - $a^{(P-1)(Q-1)n+1} \bmod PQ=a$ (フェルマーの定理より)
  - (P-1)(Q-1)に対して互いに素のeを選び
    ed mod (P-1)(Q-1)=1となるdを選ぶ
    - $ed=(P-1)(Q-1)n+1$なので$a^{ed} \bmod N=a$
      つまり全ての数はe乗してからd乗すると元に戻る
  - 公開鍵は(N,e) 秘密鍵はdとする
  - 平文mに対し暗号文$C=m^e \bmod N$
    復号は$m=C^d \bmod N$
  - P、Qが大きければNの素因数分解は困難なので
    Nやeがわかってもdはなかなか求められない

フェルマー：Pierre de Fermat

e,dは対称
↓
秘密鍵で
「暗号化」
すると
公開鍵で
「復号」
できる！

最近，Nが1024bitだと解かれそうなので2048bit程度のものを使うことに

例えば
P=3,Q=11

(P-1)(Q-1)=20
$=2^2 \times 5$

e=3とすると
3d=20n+1より
d=7

どの数を3乗しても
7乗すると
元の数に

PQ=33の剰余類群
(中文では陪集群？)

この世界の数 \ べき乗数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13
14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14
15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32

やってみよう

- 素数pとqを選ぶ：これが秘密鍵のもとになる
  p=17, q=11
- pとqを掛け合わせてNをつくる
  N = 17 × 11 = 187
- (p-1) × (q-1)と互いに素 (coprime) なeを決める
  e = 7

- ここで

  秘密鍵：p=17, q=11から作られるd

  公開鍵：N = 187, e = 7

公開鍵:N = 187, e = 7を使って暗号化する

- 暗号文Cの作り方： $C = M^e \pmod N$

- 例えば01011000（XのASCIIコード）を暗号化したいとする
- $01011000_{(2)} = 88_{(10)}$
- $C=88^7 \pmod{187}$
- 7乗の計算がちょっと大変… モジュラ算術をつかう

モジュラ：module

$7 = 1 + 2 + 4$より

$88^7 \pmod{187} = [88^1 \pmod{187} \times 88^2 \pmod{187} \times 88^4 \pmod{187}] \pmod{187}$

$88^1 = 88 \equiv 88 \pmod{187}$

$88^2 = 7744 \equiv 77 \pmod{187}$

$88^4 = 59969536 \equiv 132 \pmod{187}$

$88^7 \pmod{187} = 88 \times 77 \times 132 = 894432 \equiv 11 \pmod{187}$

- **C=11**

秘密鍵d: p=17, q=11, e = 7から求める

- 秘密鍵dの求め方：$e \times d \equiv 1 \ [\mathrm{mod}\ (p-1) \times (q-1)]$

- e=7, p=17, q=11より
  $7 \times d \equiv 1 \ (\mathrm{mod}\ 16 \times 10)$
  $7 \times d \equiv 1 \ (\mathrm{mod}\ 160)$
- ここで161/7 = 23

- **d=23**

復号化：dを使ってCを復号化する

- $M = C^d \pmod N$
- C=11, N=187, d=23より
- $M=11^{23} \pmod{187}$
- 23 = 1+ 2 + 4 + 16より
  $11^{23} \pmod{187} = [11^1 \pmod{187} \times 11^2 \pmod{187} \times 11^4 \pmod{187} \times 11^{16} \pmod{187}] \pmod{187}$
- $M \equiv 88 \pmod{187}$
- $M = 88_{(10)} = \mathbf{01011000_{(2)}}$

ここで問題です

the magic words are squeamish ossifrage

N=
114,381,625,757,888,867,669,235,779,976,146,612,010,218,
296,721,242,362,562,561,842,935,706,935,245,733,897,830,
597,123,563,958,705,058,989,075,147,599,290,026,879,543,
541

このNをpとqに素因数分解してください

この問題（正しくはp, qを使って数字の暗号文を解く）は1977年の8月に新聞に掲載された。

魔法の言葉は気難しいヒゲワシ

N=
114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541

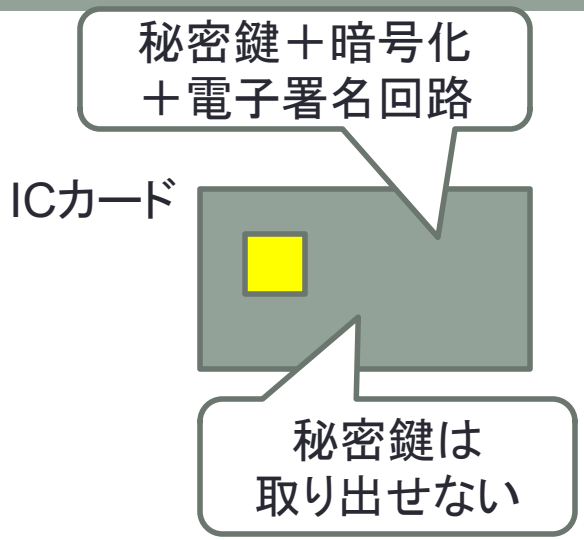
このNをpとqに素因数分解してください

この問題（正しくはp, qを使って数字の暗号文を解く）は1977年の8月に新聞に掲載された。

解読されたのは、17年後の1994年4月26日　600人のボランティアによる

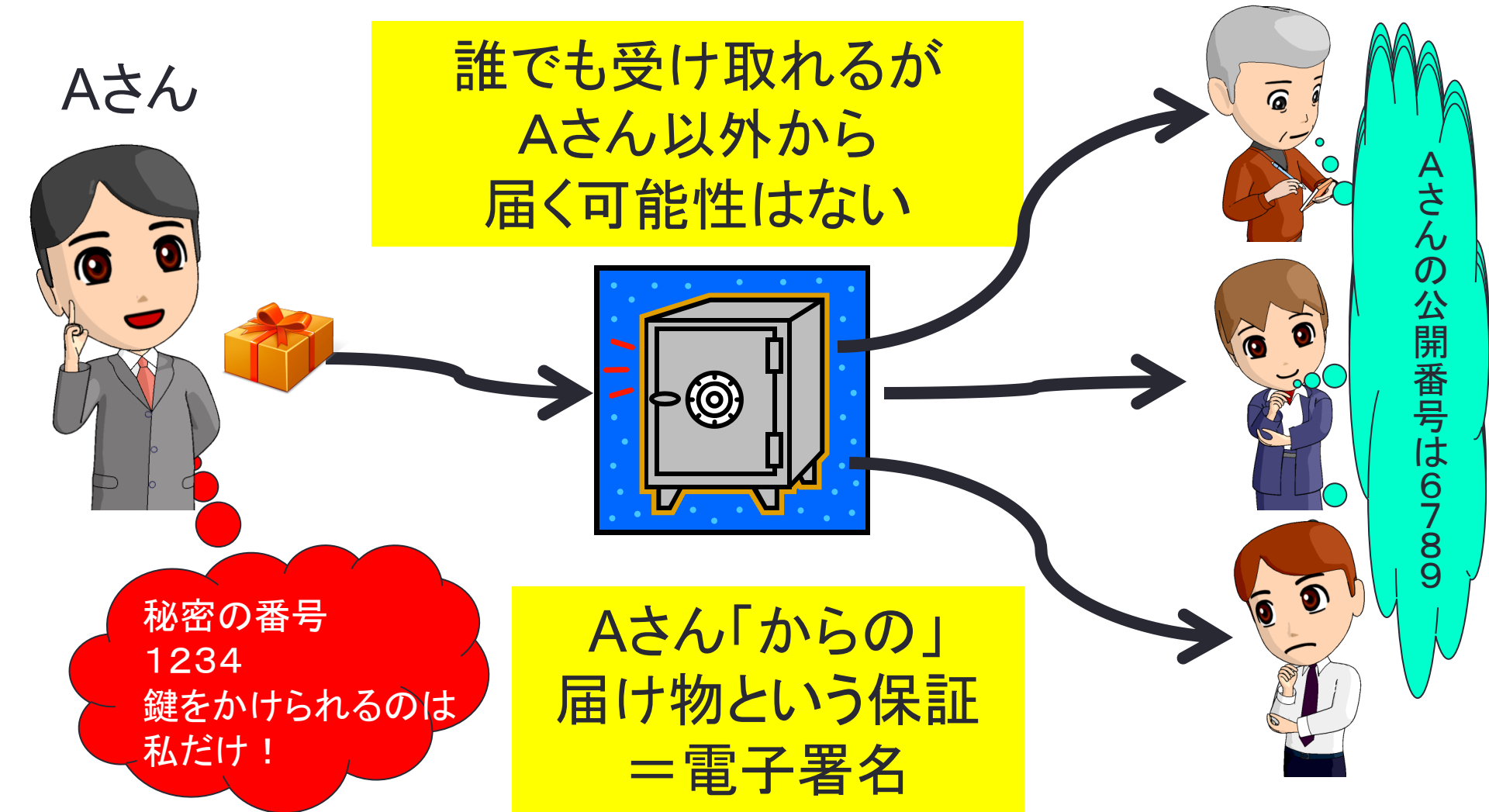
ボランティア：Volunteer

公開鍵暗号について

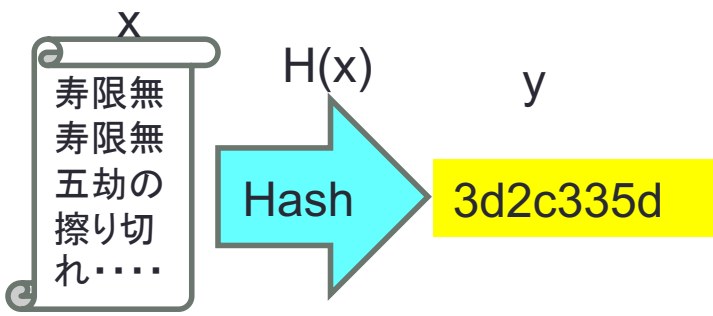


- RSA以降、いくつかの手法が発見される
  - ElGamal, 楕円曲線暗号など
- メリット
  - 公開鍵は秘匿する必要がないので容易に公開可
  - 秘密鍵は公開することがないので秘密を保ちやすい
  - N人のユーザ間での通信も鍵はN組で済む
  - 公開鍵を利用して電子署名アルゴリズムが作れる
    - たとえばRSAなら公開鍵と秘密鍵は対称なので簡単
      - 対称性のない公開鍵暗号を基にした方法はもう少し複雑
- デメリット
  - 一般に（共通鍵暗号に比べ）計算量が格段に多い＝遅い
    - 共通鍵を公開鍵で暗号化して受信者に送った後、
      その共通鍵で暗号化した暗号文を送るとよい
  - 一対多・多対多同報通信が苦手（受信者の数だけ暗号化）

RSA公開鍵を使った「電子署名」：秘密鍵で「暗号化」する

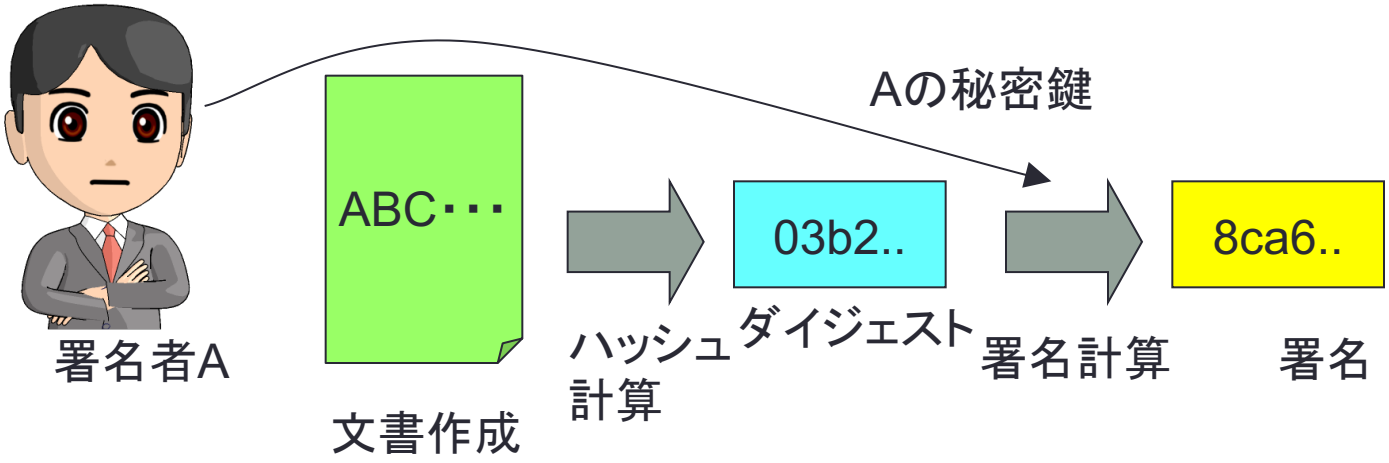


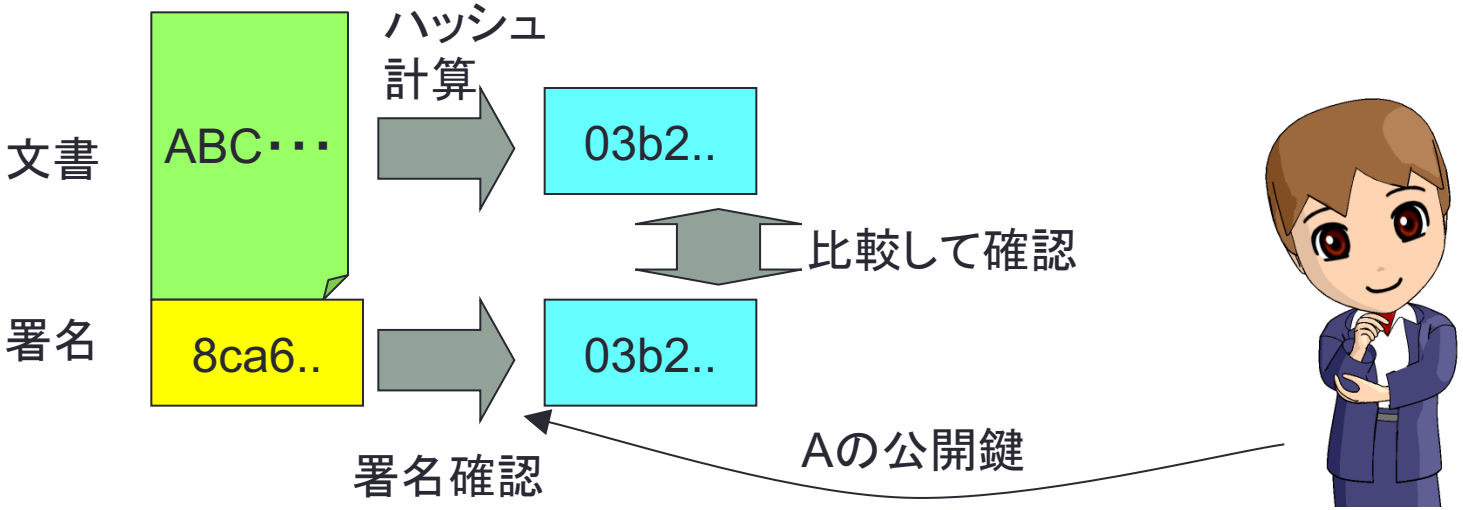
（暗号性）ハッシュ関数 (hash function)



- 任意の長さの入力データから、固定長のデータを作り出す関数
  y＝H(x) ： yはxの「ハッシュ値」
- MD5(128bit)、SHA(160～512bit)などが知られている
- yからxを求めることは困難
  - 一方向性関数（One-way function）とも呼ばれる
- あるxとyの組が判っているときにでも、同じyになる別のx'を計算/推測することが難しい
  - yの値はxの同一性を示すとみなせる
    ： 同じyの値を持てばxも同一とみなせる
    - その意味でyをMessage-digest(ダイジェスト）とも呼ぶ
    - 違うxに対して同じyが得られた時、これを衝突(Collision)と呼ぶ
- 平文全体を秘密鍵で署名するのは時間がかかりすぎるので ハッシュ関数で平文ダイジェストを得て、それに署名する

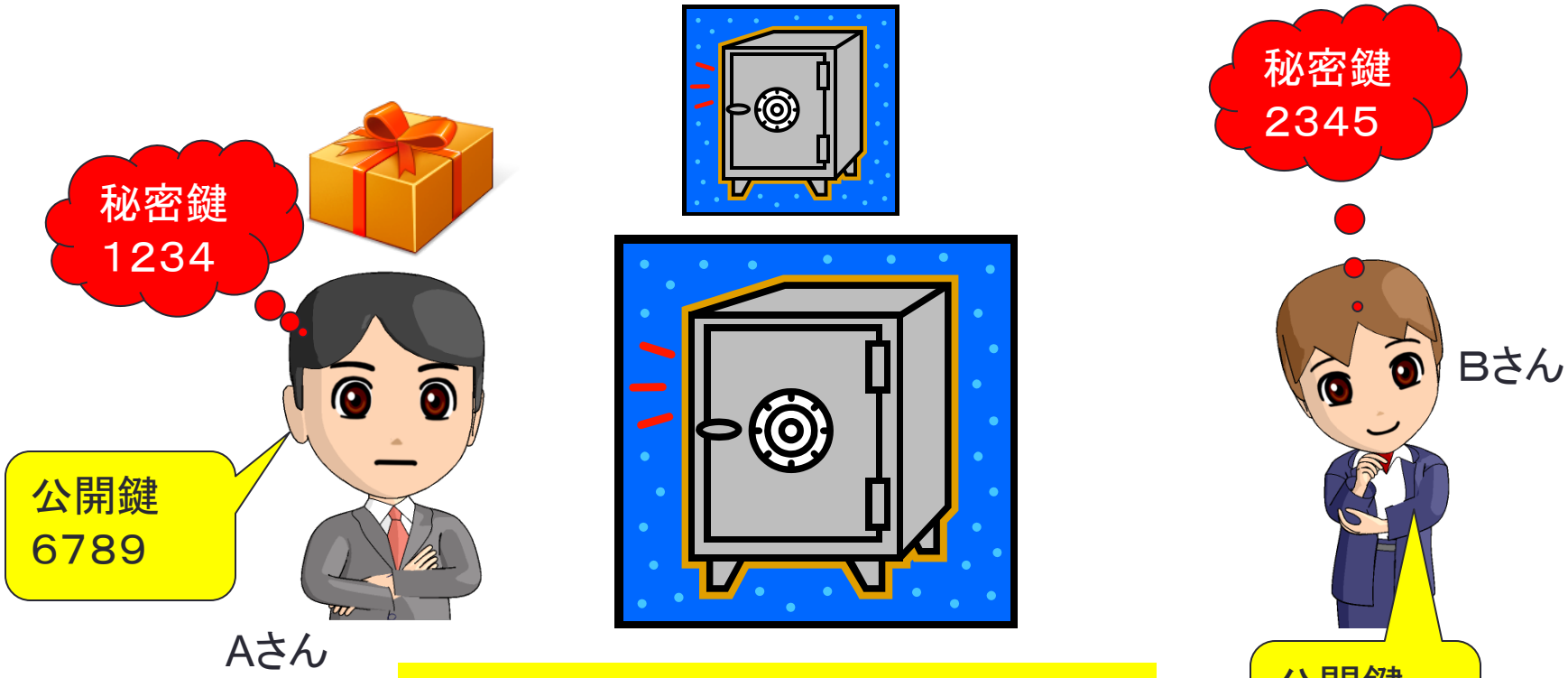
実際の電子署名の仕組み



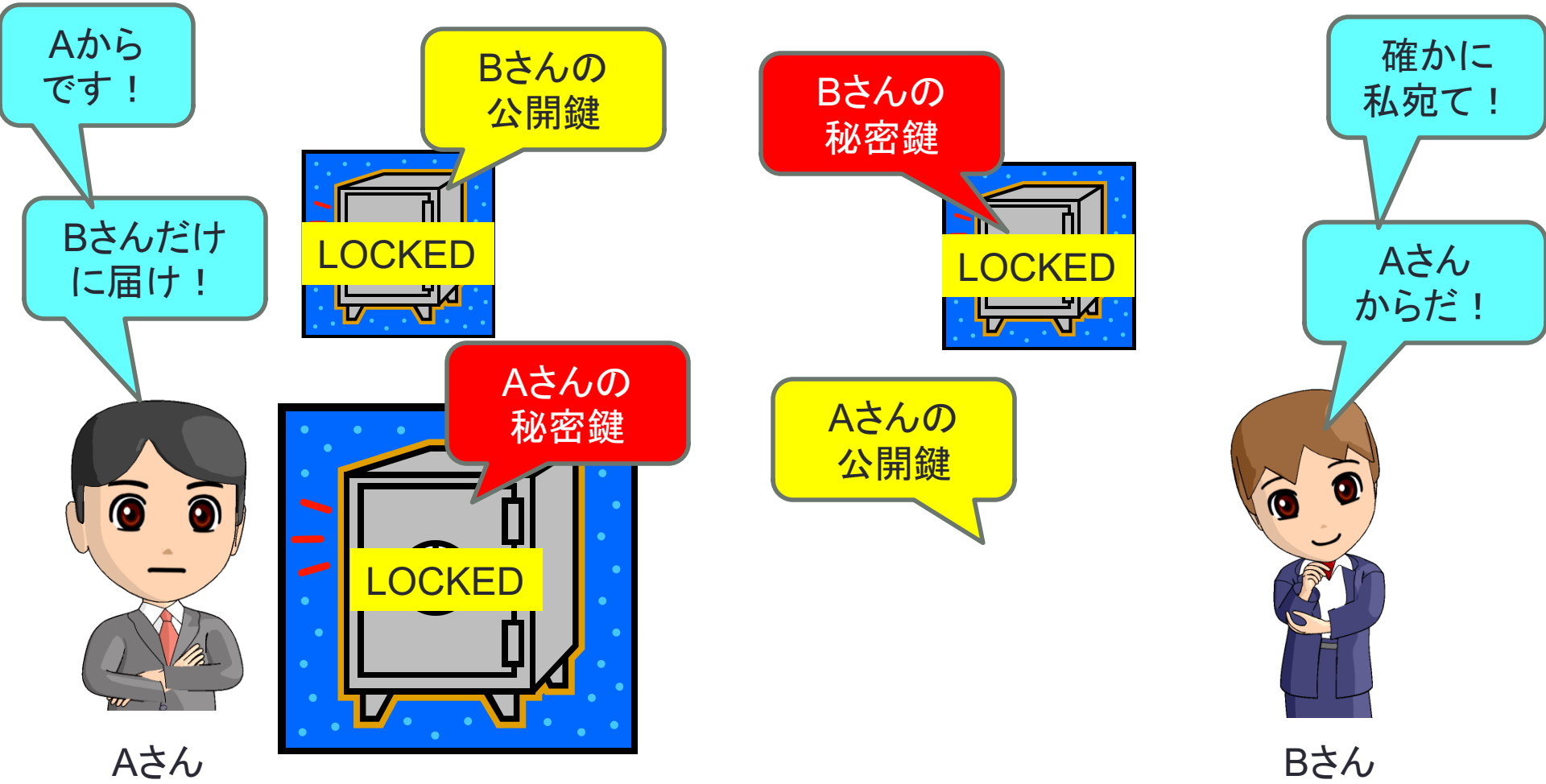


暗号化＋署名＝「認証付き通信」

- AさんからBさんに確実にモノを届けたい



暗号化してから署名


Aから
です！
Bさんだけ
に届け！
Aさん
Bさんの
公開鍵
LOCKED
Aさんの
秘密鍵
LOCKED
Bさんの
秘密鍵
LOCKED
Aさんの
公開鍵
確かに
私宛て！
Aさん
からだ！
Bさん