

情報通信を行なう際の要請

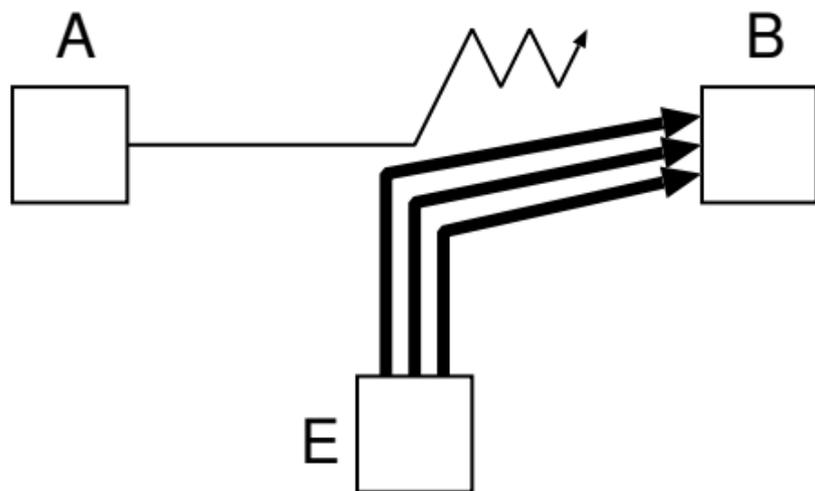
(Requirements in communication)

- 効率的に (efficiently)
→ 情報理論 (Information Theory)
- 確実に (certainly)
→ 符号理論 (Coding Theory)
- 安全に (safely)
→ 暗号理論 (Cryptography)

安全な情報伝達を阻害するもの
(obstructions for safe communication)

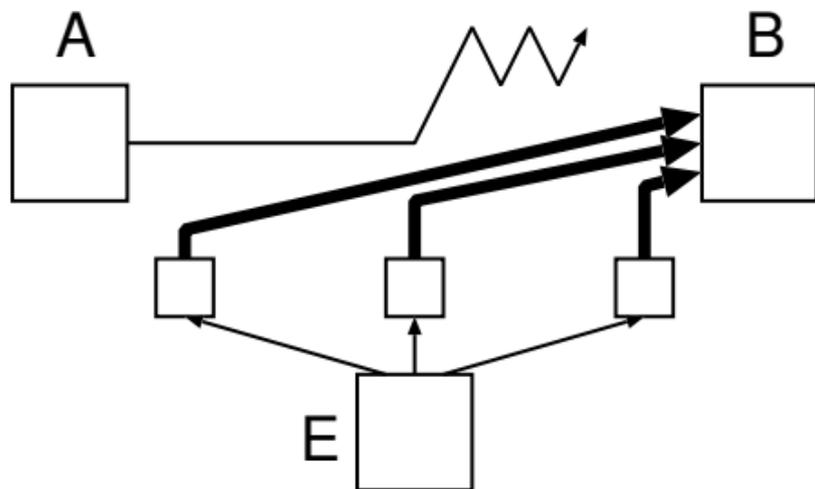
- 妨害 (obstruction) (DoS 攻撃など)
- 盗聴 (tapping)
- 改竄 (tampering)
- なり済まし (disguise) etc.

DoS 攻撃 (Denial-of-service attack)



B を機能停止に追い込むには
E に相当のマシンパワーが必要
そこで実際には …

DoS 攻撃 (Denial-of-service attack)



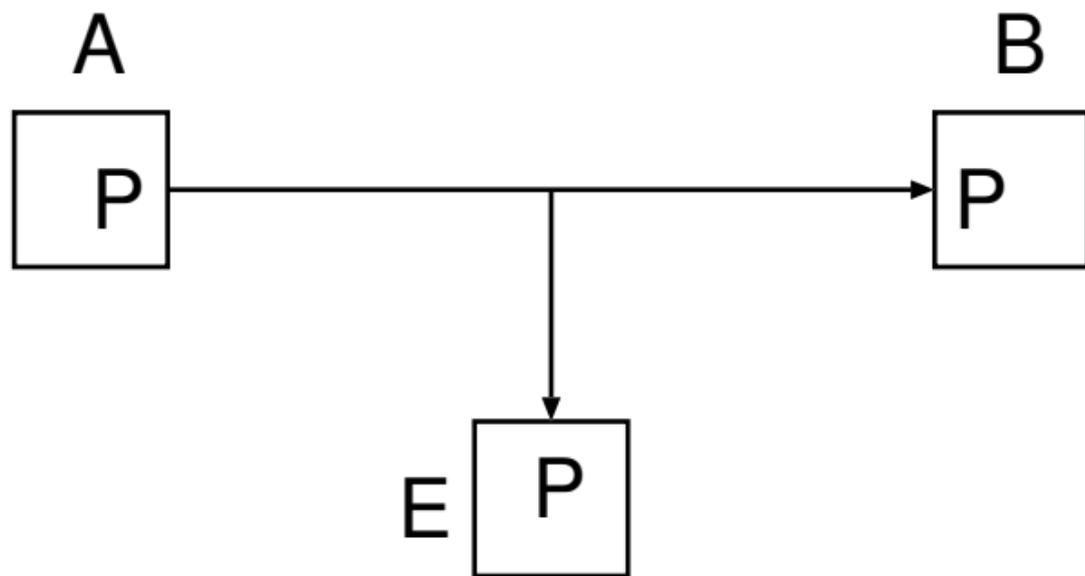
実際には、

コンピュータウイルス・乗っ取りなどで

制御下に置いた多数の機械から一斉に攻撃

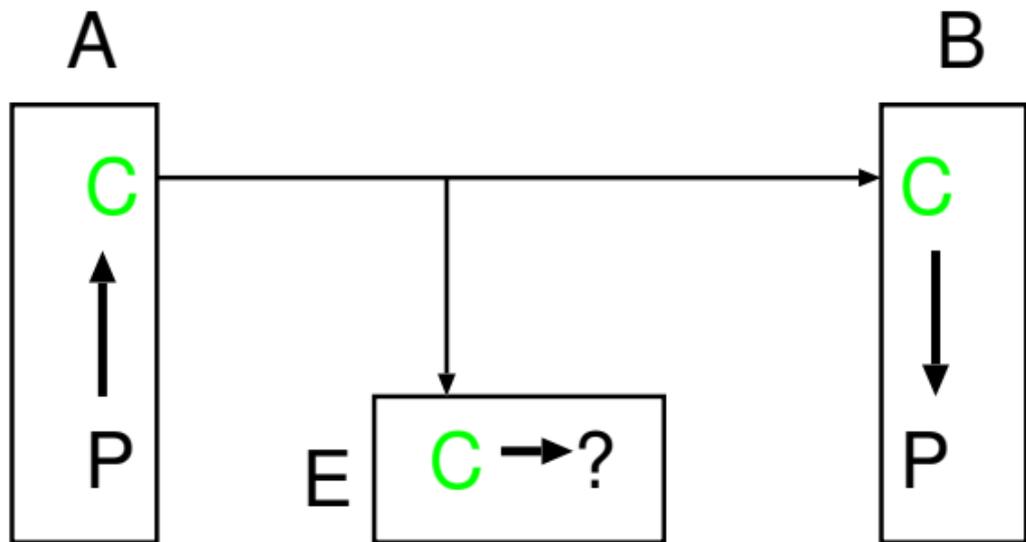
… **distributed denial-of-service attack (DDoS)**

盗聴 (tapping)



現在の計算機ネットワークの仕組みでは、
事実上、通信経路は誰にでも見られる

暗号を用いた秘匿通信 (secret communication)

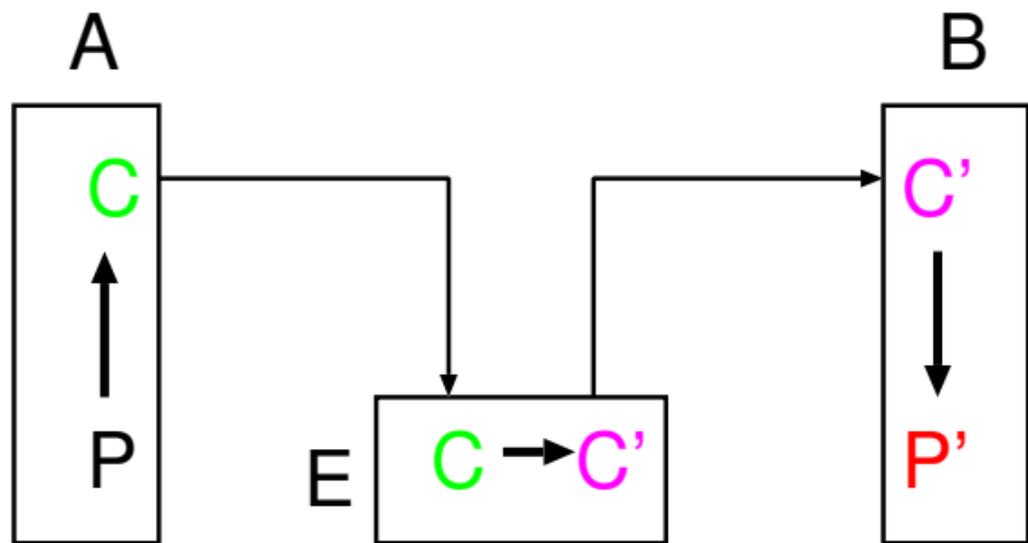


P: 平文 (plain text), C: 暗号文 (ciphertext)

P → C : 暗号化 (encryption)

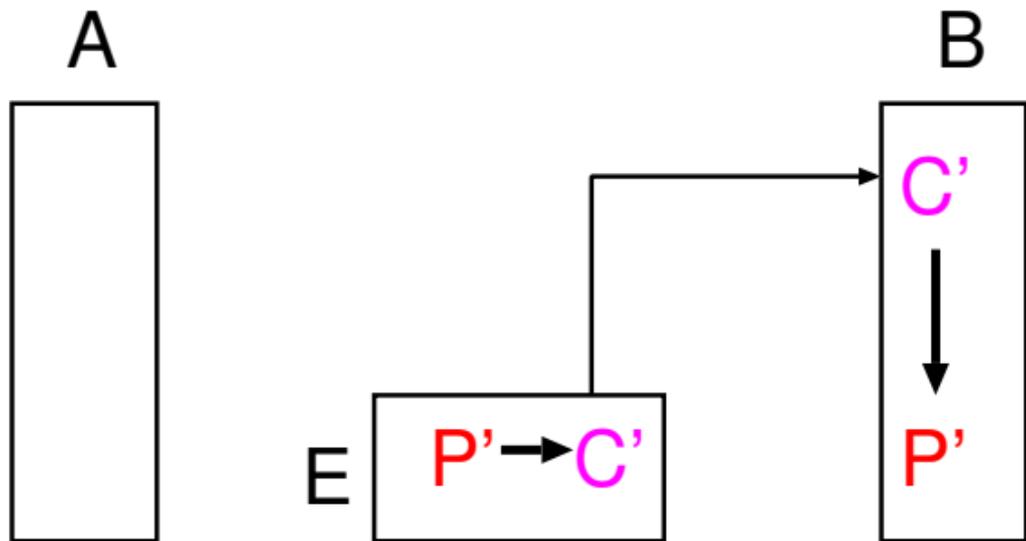
C → P : 復号 (decryption) ・ 解読 (cryptanalysis)

改竄 (tampering)



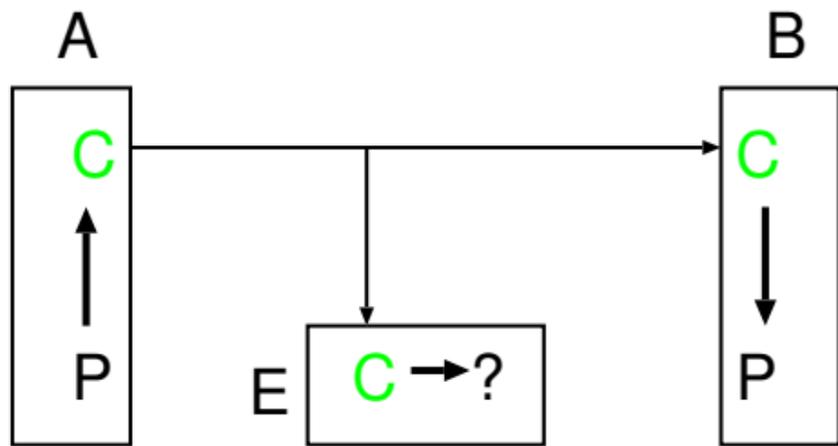
A が送信した情報であることを
確かめられるような仕組みが必要
認証 (authentication), 電子署名 (digital signature)

なり済まし (disguise)



A が送信した情報であることを
確かめられるような仕組みが必要
認証 (authentication), 電子署名 (digital signature)

暗号 (cryptography)



- 送信者 **A** が平文 **P** を暗号化、暗号文 **C** を送信
- 受信者 **B** が暗号文 **C** を受信、平文 **P** に復号
- 盗聴者 **E** は暗号文 **C** を知っても

平文 **P** を復元できない

→ **B** だけが復号鍵を持っていることが必要

暗号 (cryptography)

Assumption:

- **open channels (being tapped)**
公開された情報伝達路 (盗聴可能)
- **open cryptographic system**
暗号方式を公開
- **対称鍵暗号 (symmetric-key cryptography)**
(秘密鍵暗号・共通鍵暗号とも)
- **公開鍵暗号 (public-key cryptography)**

暗号 (cryptography)

- **共通鍵暗号 (秘密鍵暗号)**
 - ★ 送信者・受信者で同じ鍵を秘密裡に共有
 - ★ 共通の鍵で暗号化・復号を行なう

- **公開鍵暗号**
 - ★ 暗号化鍵 (公開鍵)・復号鍵 (秘密鍵) が別
 - ★ 公開された暗号化鍵を用いて暗号化
 - ★ 復号鍵は受信者だけの秘密

共通鍵暗号 (symmetric-key cryptography)

暗号化鍵・復号鍵が同じ

- **substitution ciphers (換字暗号)**
- **Caesar cipher**
- **linear block ciphers (線型ブロック暗号)**
- **Vernam ciphers (one-time pad)**
- **DES (Data Encryption Standard)**
- **AES (Advances Encryption Standard)**

Ex. Caesar cipher (Caesar 暗号)

Key (鍵) : $n \in \mathbb{Z}/26\mathbb{Z}$

Encryption (暗号化) : n -shift backward

Decryption (復号) : n -shift forward

... XYZABCDEF**GH**I**J**KLMN
 OPQRSTUVWXYZABC ...

例: $n = 3$: HELLO \longrightarrow KHOOOR

Caesar 暗号の脆弱性 (Weakness of Caesar cipher)

鍵を知らなくても容易に解読されてしまった

- 鍵の可能性が少なく、総当たりで倒せる
- 暗号文に平文の特徴が残っている

このような脆弱性を克服した暗号方式が
現在では用いられている

- **DES (Data Encryption Standard)**
- **AES (Advanced Encryption Standard)**

秘密鍵 (共通鍵) 暗号の特徴

(properties of symmetric-key cryptography)

暗号化鍵・復号鍵が同じ

The encryption key and the decryption key
are the same.

- 一般に原理は簡単で高速 (simple, fast)
- 事前の鍵共有の必要 (need key-sharing)
- 通信相手毎に別の鍵が必要
(need a different key for each pair)

現在の情報化社会では
様々な場面で暗号が使われている

例: インターネット取引 (ネットショッピングなど)

- 不特定多数の人と暗号通信をしたい
- 事前に鍵を共有できない

→ 共通鍵暗号では実現が困難

→ 公開鍵暗号・鍵共有方式のアイデア

(1976 ~ 77)

公開鍵暗号 (Public-key cryptography)

暗号化鍵 (公開鍵) ・ 復号鍵 (秘密鍵) が別

The encryption key and the decryption key
are different.

- 事前の鍵共有の必要無し
(No need key-sharing in advance)
→ 見ず知らずの人からも送ってもらえる
- 認証 (authentication) ・ 署名 (signature)
の機能がある
→ 改竄・なり済ましの対策
→ 否認防止 (non-repudiation) の機能も持つ

公開鍵暗号 (Public-key cryptography)

但し、一般には、

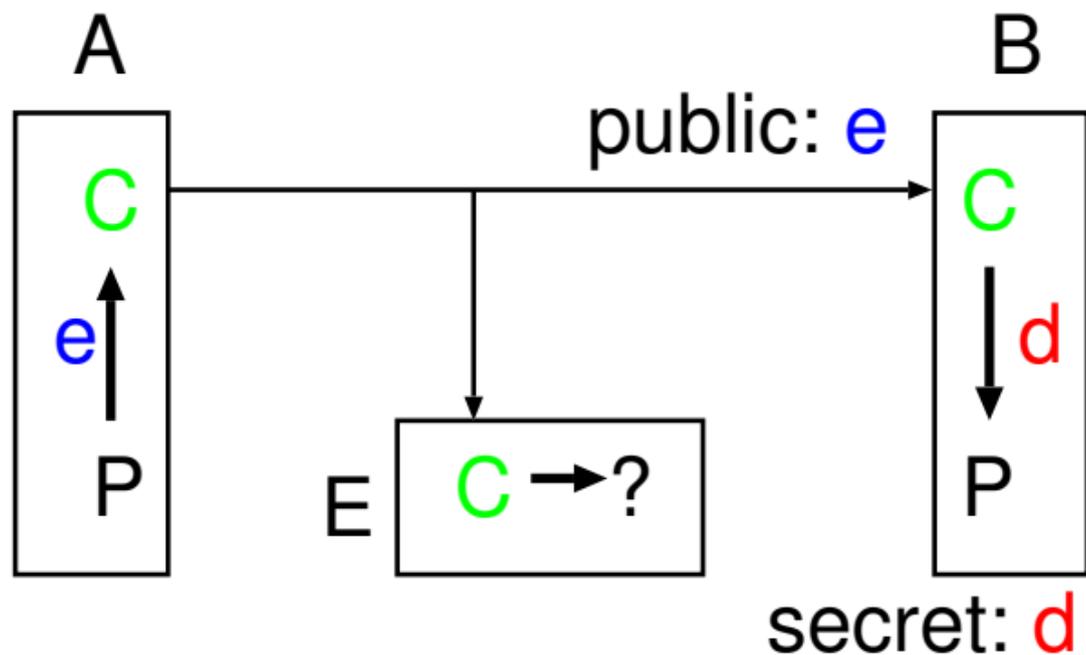
暗号化・復号が共通鍵暗号に比べて低速 (slow)

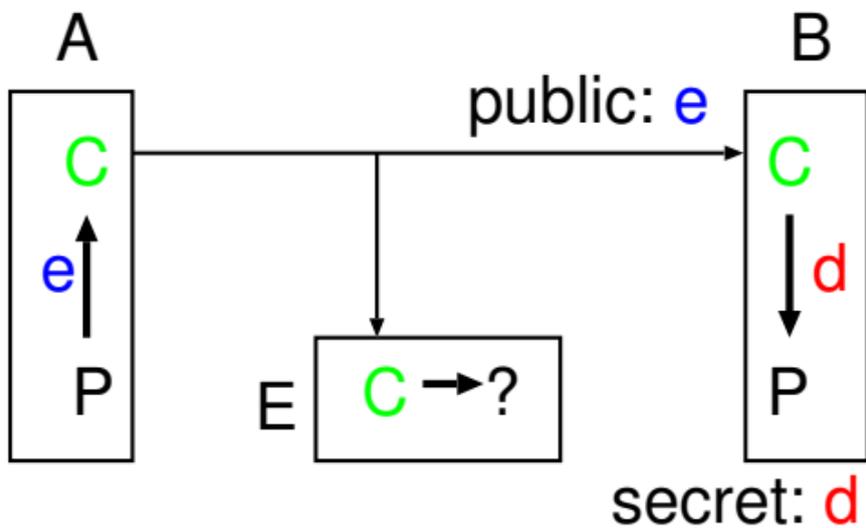
そこで、

- 始めに公開鍵暗号方式で鍵を送付・共有
(first share a secret key
under public-key cryptosystem)
- その鍵を用いて秘密鍵暗号方式で通信
(then communicate with the key
under secret-key cryptosystem)

というように、組合わせて用いることが多い

公開鍵暗号による暗号通信



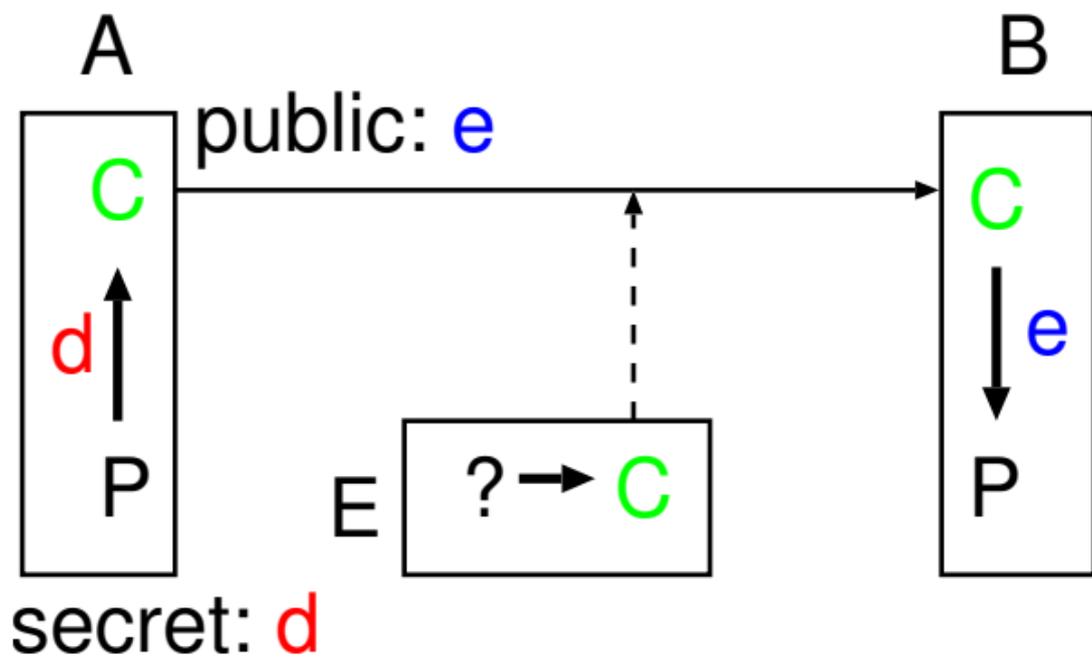


しかし、これだと誰でも暗号化できるので、

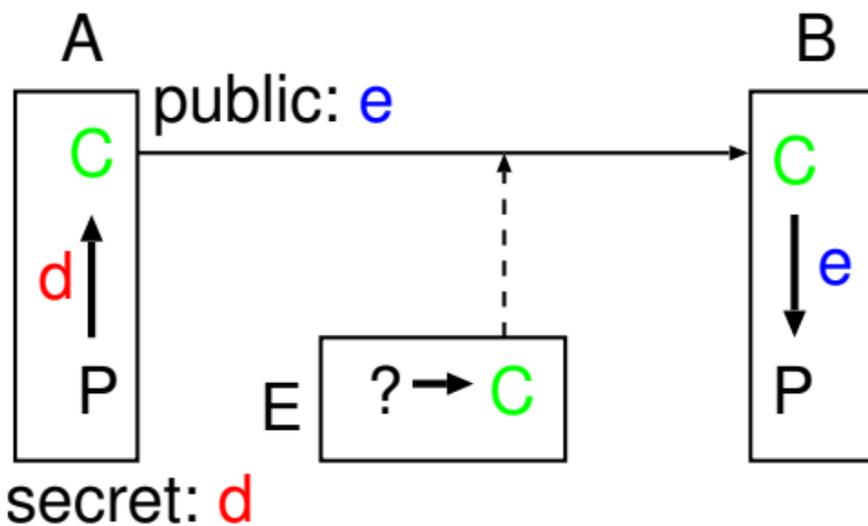
A 氏が送った保証がない

→ 署名 (signature) の必要性

公開鍵暗号を用いた署名 (signature)



公開鍵暗号を用いた署名 (signature)



盗聴者 E 氏は

平文 P は判らないが、暗号文 C は盗聴可能

→ いつも同じ署名は使えない

公開鍵暗号を用いた署名 (signature)

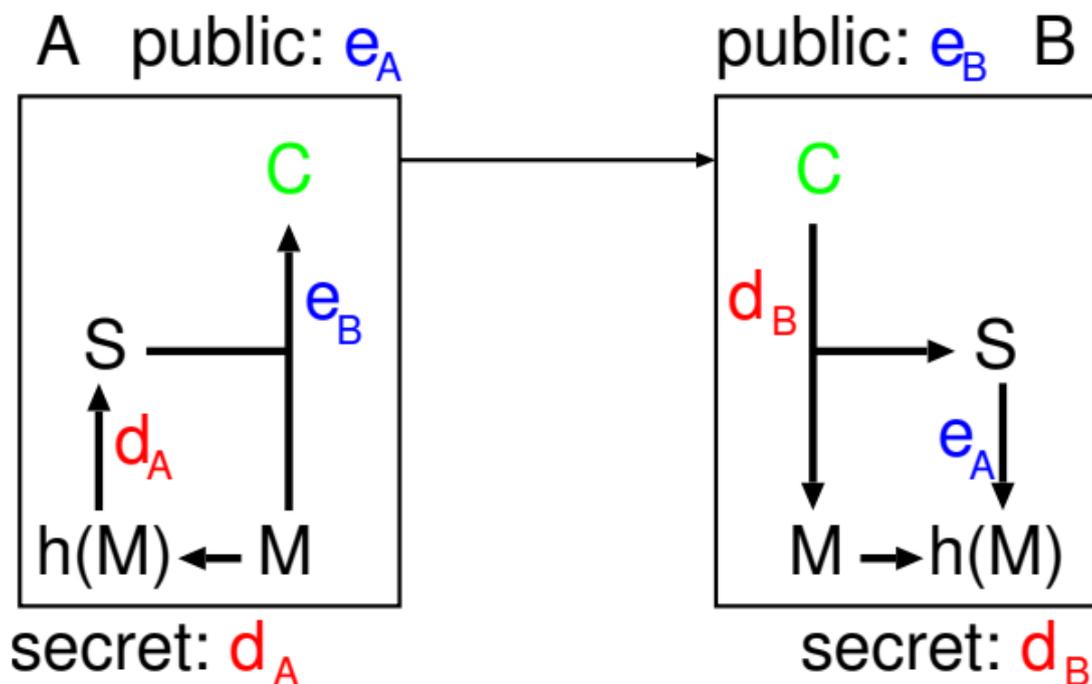
実際には、メッセージ本文 M に対して、

M から決まる短い値 (hash value) $h(M)$ を

送信者 **A** 氏の秘密鍵で暗号化した文字列 S を
本文 M に添付して、

受信者 **B** 氏の公開鍵と一緒に暗号化して送る

公開鍵暗号を用いた署名 (signature)



公開鍵暗号の特徴

(properties of public-key cryptography)

- 暗号化は誰でも出来る
(Everyone can encrypt.)
- 復号は秘密鍵を知らないと出来ない
(Decryption requires the secret key.)
(もの凄く時間が掛かる)

そんな都合の良い仕組みが本当にあるのか？

→ ある!! (多分大丈夫)

公開鍵暗号の特徴

(properties of public-key cryptography)

- 暗号化は誰でも出来る
(Everyone can encrypt.)
- 復号は秘密鍵を知らないと出来ない
(Decryption requires the secret key.)
(もの凄く時間が掛かる)

計算困難な問題 を利用

(use of problems hard to compute)

- 素因数分解 (prime decomposition)
- 離散対数問題 (discrete logarithm)

代表的な公開鍵暗号方式

(public-key cryptosystems)

- **RSA cryptosystem**
(Rivest-Shamir-Adleman)
- **Diffie-Hellman key-exchange** (鍵共有)
- **ElGamal encryption**

公開鍵暗号の例: RSA 暗号

Rivest, Shamir, Adleman (1977)

- 大きな素数 p, q を選び、積 $n = pq$ を作る
- n を用いて、公開鍵 e ・秘密鍵 d の対を作る
- 暗号化の計算は n と公開鍵 e とから可能
- 復号は秘密鍵 d を用いる
- n と公開鍵 e とから秘密鍵 d を求めるには、 n の素因子分解 $n = pq$ が必要
- しかしそれは困難 (膨大な計算時間が掛かる)