

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

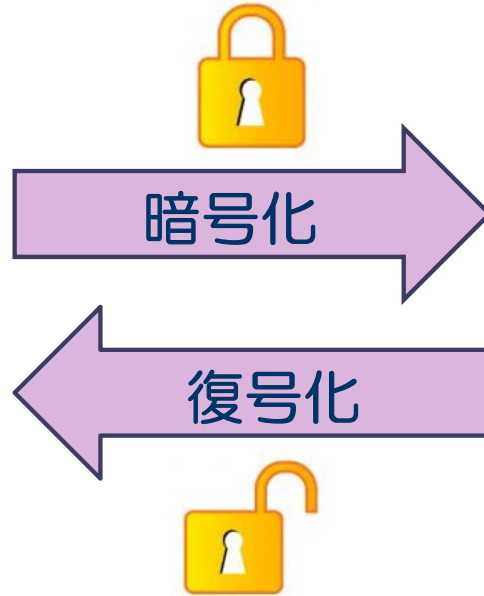
- 当事者以外には秘密にしておきたい情報を送るときに使う方法
- 当事者だけが、平文に鍵をかける方法、暗号文の鍵を解く方法を知っている（はず）。
- 暗号の歴史：暗号開発者と暗号解読者の知恵比べの歴史

RSA暗号は次のような方式である：鍵ペア（公開鍵と秘密鍵）を作成して公開鍵を公開する。まず、適当な正整数 e （通常は小さな数。65537 = $2^{16} + 1$ ）がよく使われる）を選択する。また、大きな2つの素数 $\{p, q\}$ を生成し、それらの積 $n (= pq)$ を求めて、 $\{e, n\}$ を平文の暗号化に使用する鍵（公開鍵）とする。2つの素数 $\{p, q\}$ は、暗号文の復号に使用する鍵（秘密鍵） d の生成にも使用し、秘密に保管する。

暗号化（平文 m から暗号文 c を作成する）：
復号（暗号文 c から元の平文 m を得る）：
ここで、暗号化（ e 乗）は、 $\{e, n\}$ があれば容易に計算できるのに対して、復号（ e 乗根）は、「 n の素因数を知らない」と難しい（大きい合成数の素因数分解も難しい）」と考えられている。つまり秘密鍵を用いずに暗号文から平文を得ることは難しい、と信じられている。これがRSA暗号の安全性の根拠である。

RSA暗号のアルゴリズムは、1983年9月20日にアメリカ合衆国で特許（4,405,829号）を取得し、RSA Security 社がライセンスを独占していたが、特許期間満了に伴って2000年9月6日からは誰でも自由に使用できるようになった。

平文
(ひらびん, plain text)



```
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
#!/ d*a<a?=1%7+1*d<h$z?
```

第三者が見ても
分からない

暗号文
(cryptogram)

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	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。

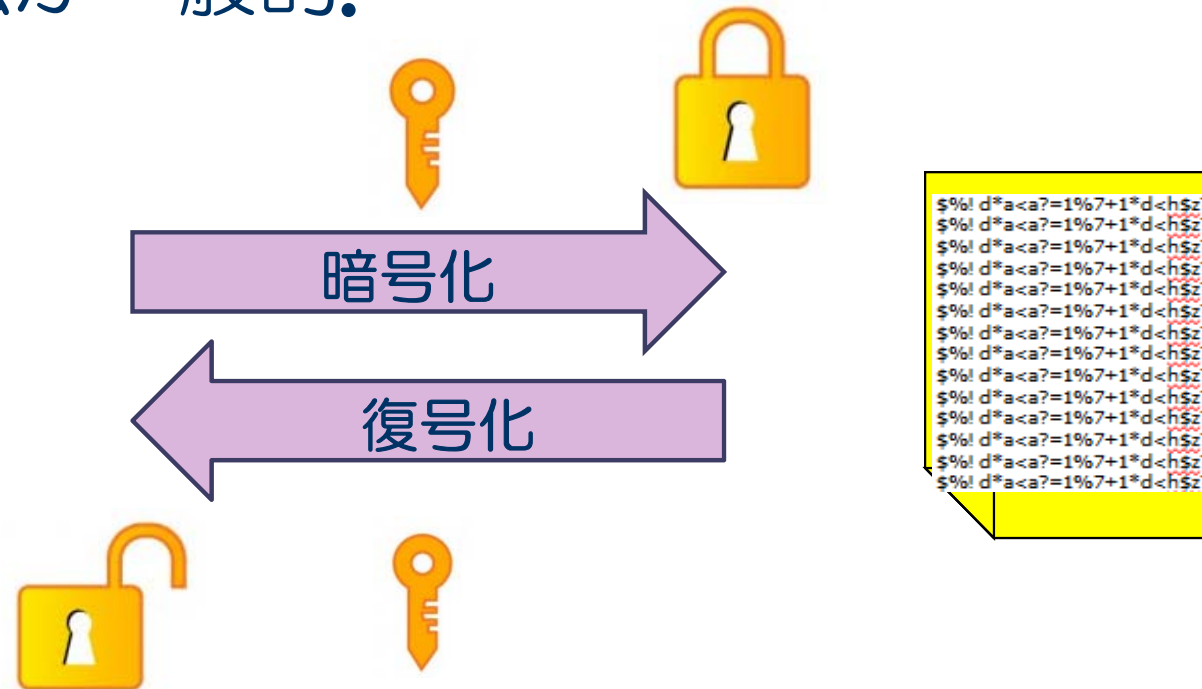
暗号のポイント

- 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。

RSA暗号は次のような方式である：鍵ペア（公開鍵と秘密鍵）を作成して公開鍵を公開する。まず、適当な正整数 e （通常は小さな数、 $(65537 = 2^{16} + 1)$ がよく使われる）を選択する。また、大きな2つの素数 $\{p, q\}$ を生成し、それらの積 $n (= pq)$ を求めて、 $\{e, n\}$ を平文の暗号化に使用する鍵（公開鍵）とする。2つの素数 $\{p, q\}$ は、暗号文の復号に使用する鍵（秘密鍵） d の生成にも使用し、秘密に保管する。

暗号化（平文 m から暗号文 c を作成する）：
復号（暗号文 c から元の平文 m を得る）：
ここで、暗号化（ e 乗）は、 $\{e, n\}$ があれば容易に計算できるのに対して、復号（ e 乗）は、 $\{n$ の素因数を知らないと難しい（大きい合成数の素因数分解も難しい）と考えられている。つまり秘密鍵を用いずに暗号文から平文を得ることは難しい、と信じられている。これがRSA暗号の安全性の根拠である。

RSA暗号のアルゴリズムは、1983年9月20日にアメリカ合衆国で特許（4,405,829号）を取得し、RSA Security 社がライセンスを独占していたが、特許期間満了に伴って2000年9月6日からは誰でも自由に使用できるようになった。

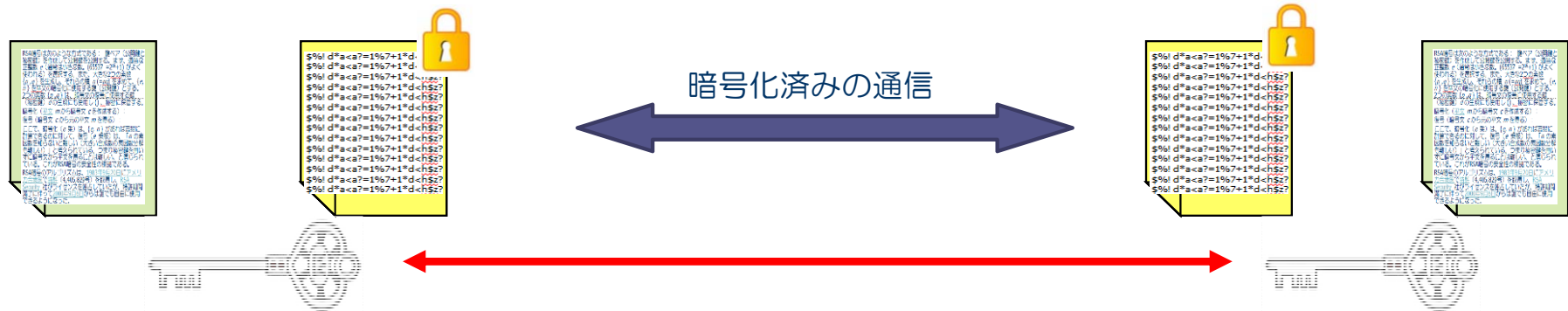


共通鍵暗号方式

- 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.

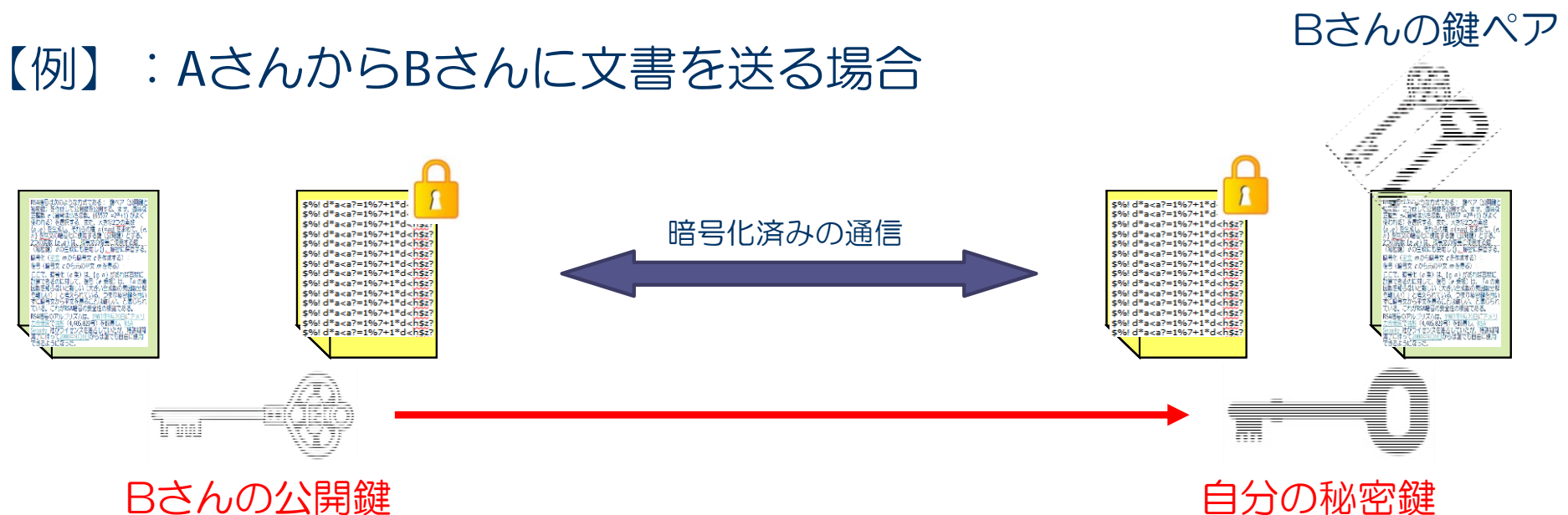


- 相手にどのように鍵を渡すか?
 - ① 暗号化しないで送る.
⇒ 鍵が盗聴されたら, 暗号化の意味がない.
 - ② 直接会って伝える.
⇒ 鍵を定期的に変える場合など面倒. 遠い相手には不便.
 - ③ 盗聴されないような方法 (開封が分かる郵送等) で伝える.
⇒ 不特定多数への相手に送るのは現実的でない.

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

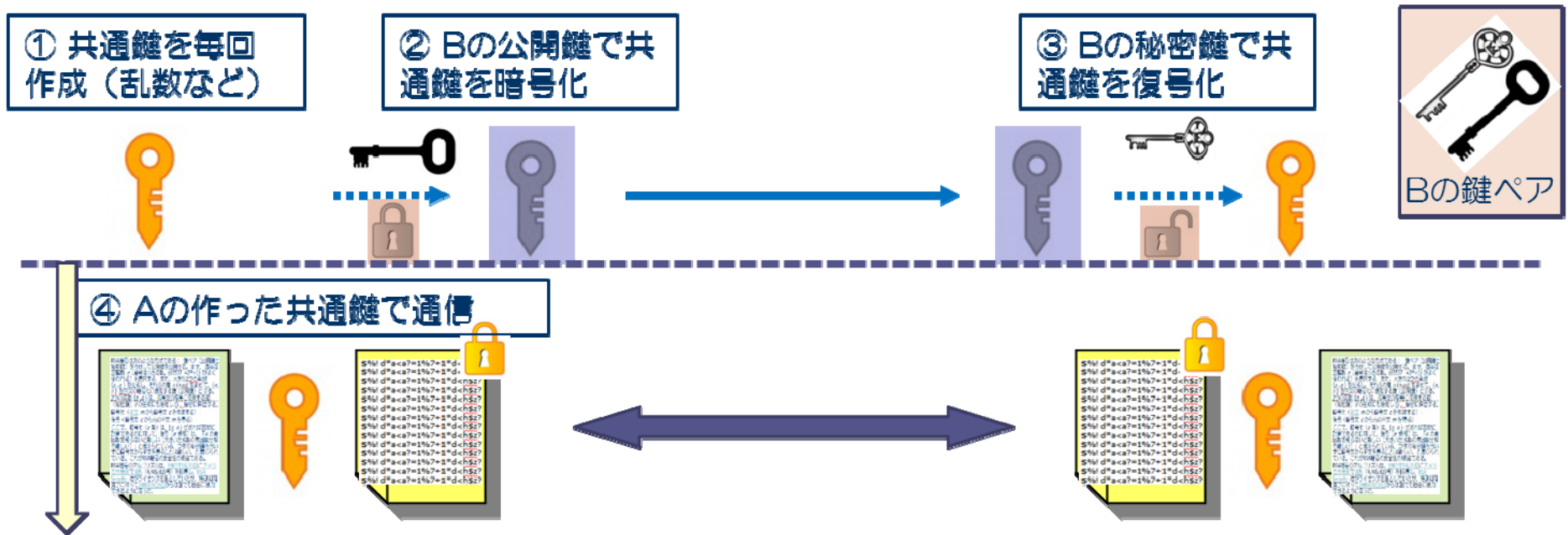
- ◆ 安全な鍵の配送を実現した。
 - 公開鍵だけ相手に送れば良い。
- ◆ 鍵の管理の負担を軽減した。
 - 秘密に管理すべきは自分の秘密鍵だけ。

■ 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。

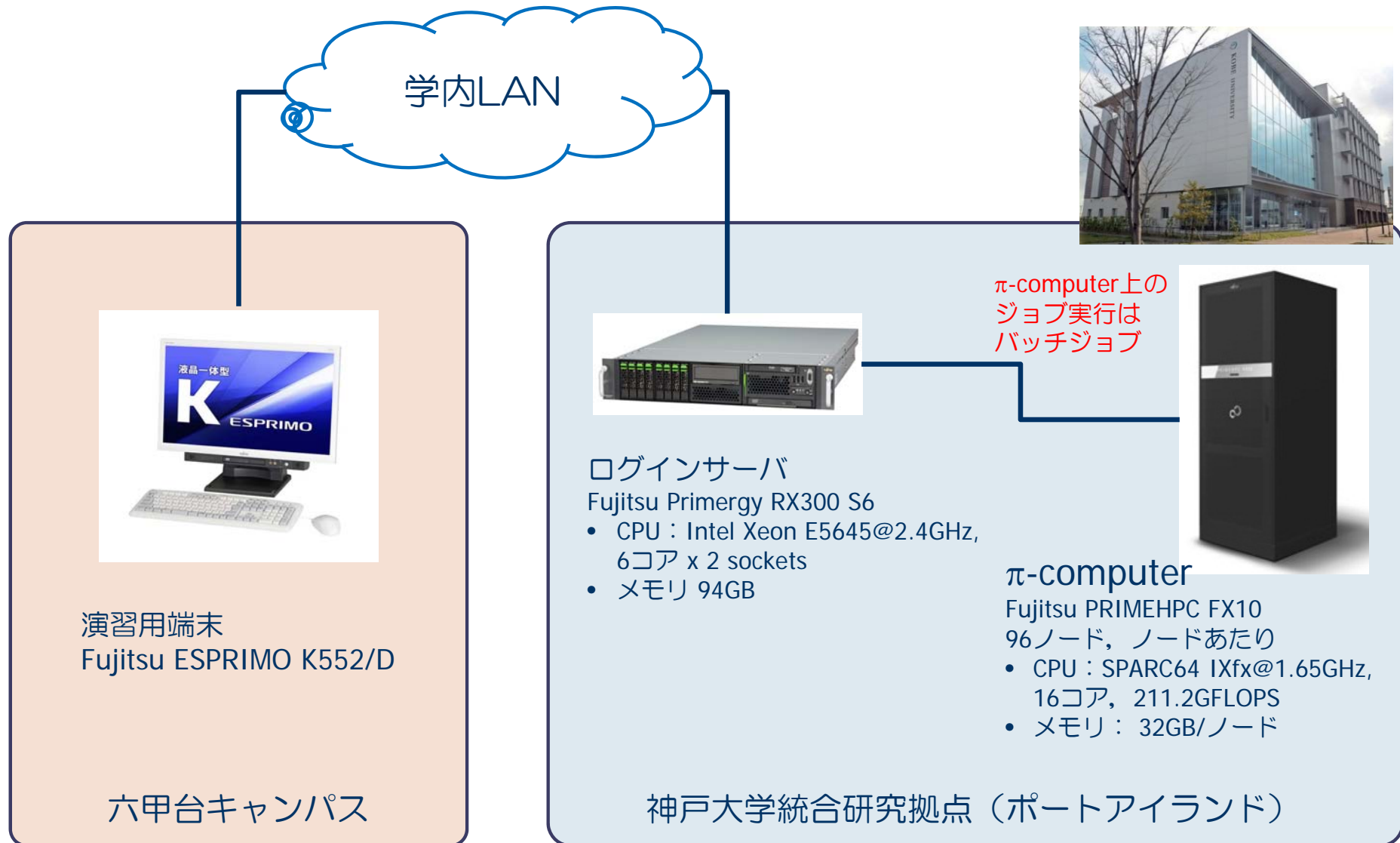


- 利点

- ◆ 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。

π -computerにアクセス

計算科学演習A1, A2で使用するスパコン



π -computerにアクセスするための手順

- (1) 演習室端末にログインする。
- (2) ブラウザを立ち上げ，演習用ページを見る。
 - ① 演習室端末用のパスワードを変更する。
 - ② 仮の秘密鍵をデスクトップにコピーする。
- (3) MobaXtermを起動する。
 - ① 自分の鍵ペア（秘密鍵，公開鍵）を作成する。
 - ② 仮の秘密鍵を使って， π -computerにログインする。
 - ③ 自分で作成した公開鍵を，登録する。
 - ④ 自分の鍵ペアでログインできることを確認
 - ⑤ 仮の公開鍵を削除

(1) 演習室端末にログインする.

■ ユーザID

◆ 修士学生 : m999x999

m, xは小文字, 999x999は学籍番号にする.

◆ 学部学生 : t9999999

tは小文字. 9999999は学籍番号にする.

■ 初期パスワード : cp20180412

(2) ブラウザを立ち上げ，演習用ページを見る。

- 計算科学演習のwikiページ

http://exp.cs.kobe-u.ac.jp/wiki/comp_practice/

- パスワードを変更する。

- 仮の秘密鍵をデスクトップにコピーする。

- ◆ エクスプローラで，**¥¥vid02¥work** を開く。

- ◆ ファイル **temp_key** をデスクトップにコピーする。

(3) MobaXtermを立ち上げる.

- 自分の鍵ペア（秘密鍵，公開鍵）を作成する.
 - ◆ 演習用ページ：“ログインについて”を見ながら，各自作業する.
- 仮の秘密鍵で，ログインサーバにログイン
 - ◆ 以下，演習ページの公開鍵の登録をみて，自分の公開鍵を登録する.
- 自分の秘密鍵でログインできることを確認.
- 仮の公開鍵を削除