Webを支える情報通信技術(９)
～ 暗号技術 ～

佐藤周行、中山雅哉、西村健

先週の復習

- アクセス制御の方法を学んだ
  - IPアドレスによる制御、ドメイン名による制御
  - 人に対する制御（ID&パスワード）

  - 通信は盗聴される危険性がある！

今週の内容

- 盗聴を防ぐための暗号技術あれこれ
  - 共通鍵暗号
  - 公開鍵暗号
  - ハッシュ関数
- さらっと流すので興味があれば各自で調べてほしい

今回の話はHTTPの盗聴防止に限った話ではなく、メールなどの盗聴／改竄防止にも使われている

悪者の存在

- インターネット上にはいろんな悪さをしようとする悪者が存在することを意識しておくことが重要
  - 盗聴、改竄、なりすまし etc.

これは暗号か？

QWxhZGRpbjpvcGVuIHNlc2FtZQ==

暗号に必要なこと(1)

用語

- 元の文:平文
- 平文を別の形に変えること:暗号化
- 別の形:暗号文
- 暗号文を平文に戻すこと:復号

暗号に必要なこと(2)

- 通信相手(例:Webサーバ)のみが復号できること
  - つまり、第三者が暗号文から平文を推定すること(解読)が困難であること

インターネット上のやりとりの場合は特に

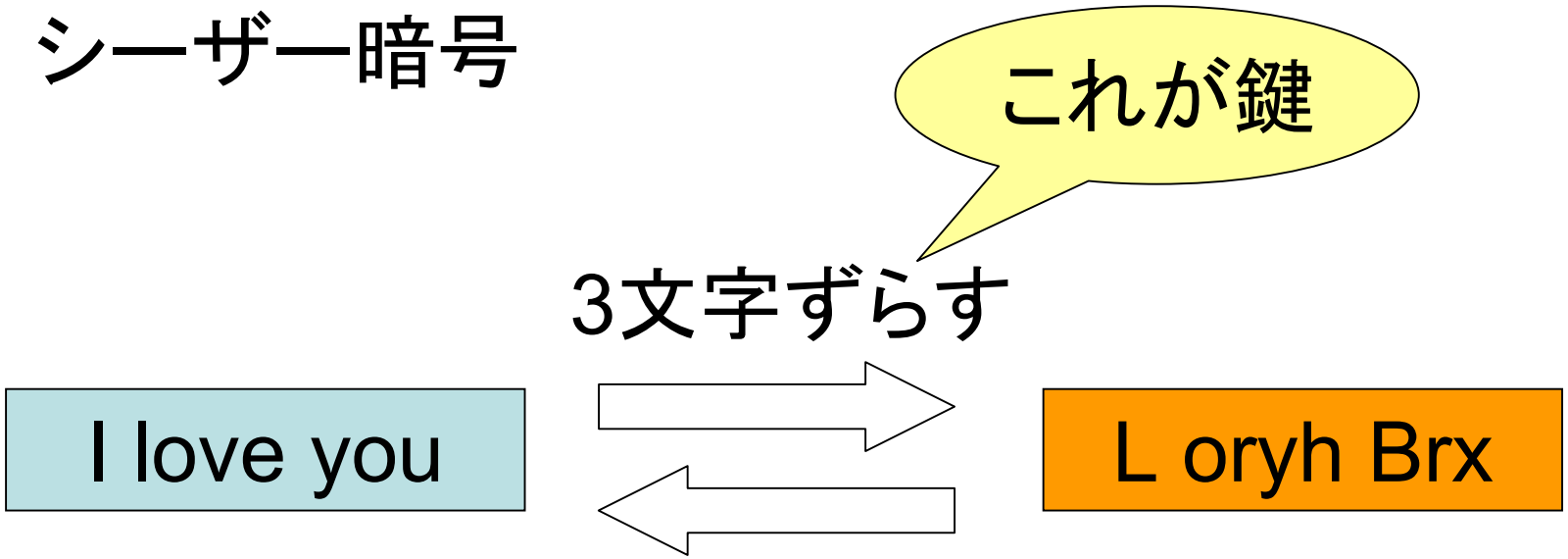
- 暗号化／復号アルゴリズムが公開されていること

- 先の暗号文はBase64(RFC 3548)という方式で暗号化されているという情報があればだれでも復号（解読）可能
  → 不適！（暗号ではない）

- アルゴリズムは公開してその他の秘密情報を二者で共有するという方法が一般的
  – 秘密情報のことを「鍵」という

共通鍵暗号

- シーザー暗号



- 実際のアルゴリズムはもっと複雑
  - DES(FIPS 46-3、古い)、AES(FIPS 197)など

演習：共通鍵暗号を使ってみよう(1)

- 「I love you.」という文をDES暗号化してファイルに保存する

```
$ openssl des > encrypted.txt
enter des-cbc encryption password:
Verifying – enter des-cbc encryption password:
I love you.
[Control + D]
```

鍵を2回入力する

Controlキーを押しながらDキーを押す

- 上で保存したファイルを復号する

```
$ openssl des –d < encrypted.txt
enter des-cbc decryption password:
…
```

鍵を入力する

演習：共通鍵暗号を使ってみよう(2)

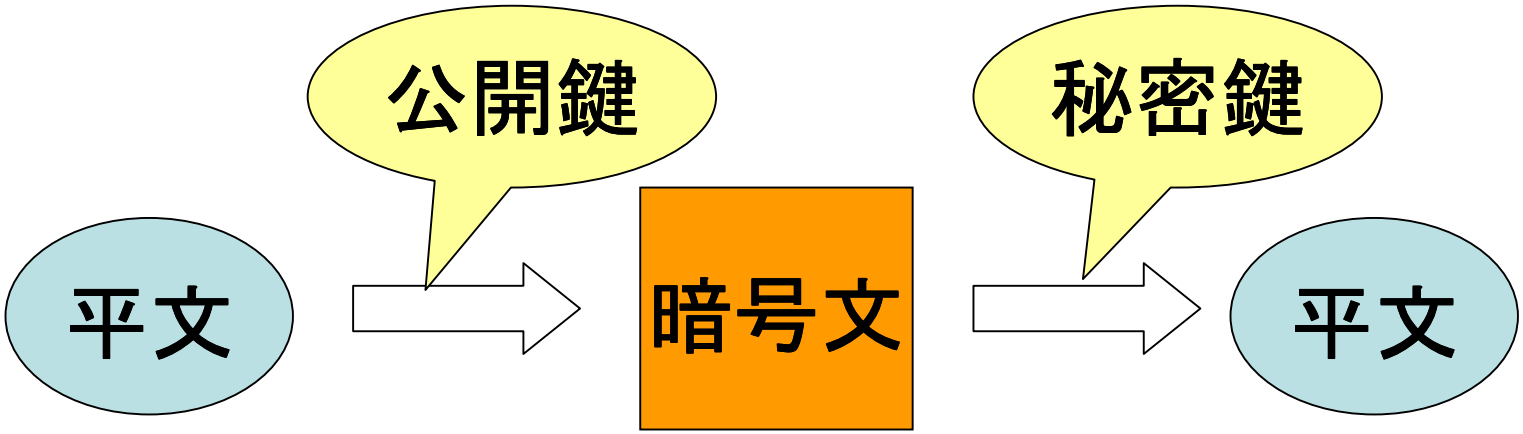
- Safariで
  `http://www-sato.cc.u-tokyo.ac.jp/PKI-project/Komaba/des2.txt`
  を開き「ファイル」→「別名で保存」で保存する

```
$ openssl des -d < Desktop/des2.txt
...
```

鍵の受け渡しってどうするの？

公開鍵暗号

- 2種類の鍵（鍵ペア）を使用する



- 公開鍵で暗号化された暗号文は対応する秘密鍵でしか復号できない
- 公開鍵を公開しておいて、暗号化に利用してもらう
- アルゴリズム：RSAなど
- RSA暗号の論文：R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.

演習：公開鍵暗号を使ってみよう(1)

- 鍵ペア（秘密鍵と公開鍵）を生成する

```
$ openssl genrsa 1024 > testkey.key
…
$ openssl rsa –pubout < testkey.key > testkey.pub
…
```

- 「abc*[改行]*」という文をRSA暗号化／復号する

```
$ openssl rsautl –inkey testkey.pub –pubin
 –encrypt > rsa.txt
…
abc
[Control+D]
$ openssl rsautl –inkey testkey.key –decrypt < rsa.txt
…
```

一行で書くこと

演習 : 公開鍵暗号を使ってみよう(2)

- 鍵の内容の確認方法

```
$ openssl rsa –text –noout < testkey.key…
```

- Safariで
  `http://www-sato.cc.u-tokyo.ac.jp/PKI-project/Komaba/testkey.pub`
  を開き「ファイル」→「別名で保存」で保存する

- RSA暗号化してみよう
- 復号ができないことを確認してみよう！