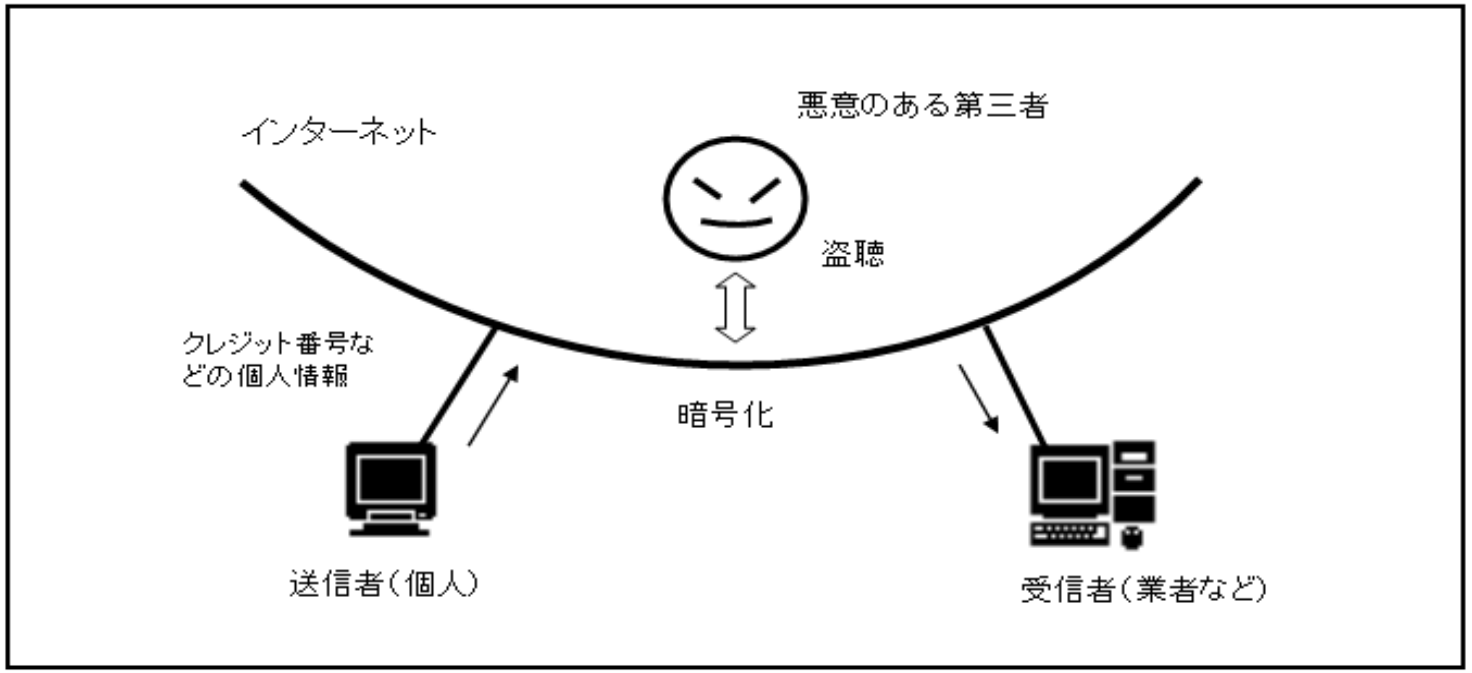
高校生のための公開鍵暗号入門

データの暗号化の必要性

第三者による盗聴の危険性



インターネット上におけるデータの暗号化技術

ネットワーク上のおける情報を暗号化して送受信するプロトコル

・SSL（Secure Socket Layer）
・TLS（Transport Layer Security）
・HTTPS（Hyper Text Transfer Protocol Secure）

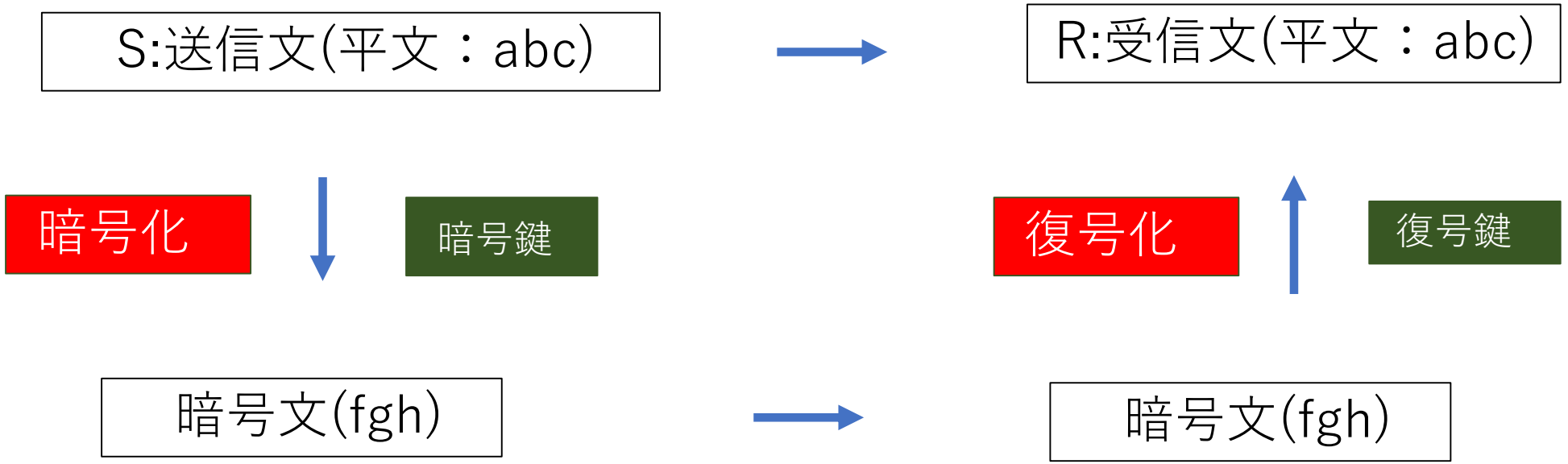
ネットワーク上でセキュリティが必要な情報

・ログイン用ID,パスワード
・ネットショッピングでの個人情報
・Webアンケートでの個人情報
・その他

日経PCEduへ

暗号方式

暗号の仕組み



暗号化の種類

・共通鍵方式　・公開鍵方式

暗号の種類と歴史

種類

・換字方式
・置換方式
・転置方式
・挿入方式　など

歴史

・シーザー暗号
・上杉暗号
・言葉の置き換え
・隠し文字
・エニグマ暗号
・いろは歌
・蜘蛛の経路
・旧日本軍の暗号など

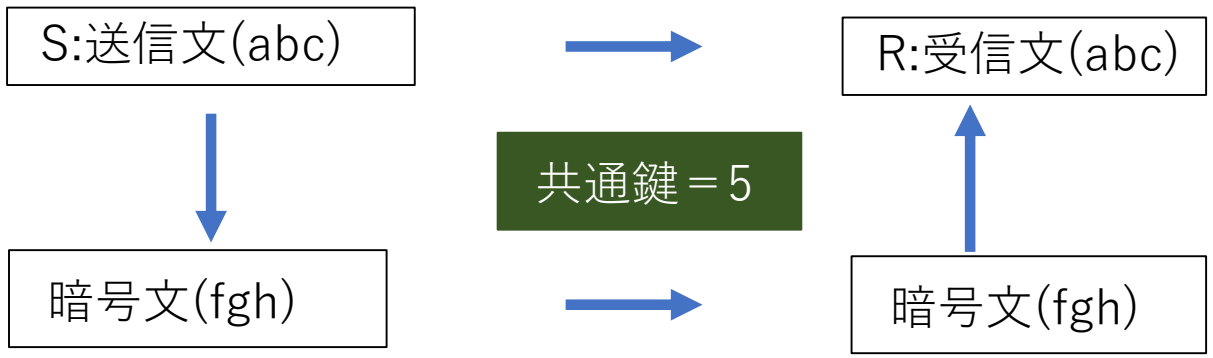
課題レポート

・歴史上の暗号化技術を2つ選んでその仕組みを説明する。
・インターネット上の暗号化技術についてまとめる。

日経PCEduへ

公開鍵暗号方式（高校生のための）

共通鍵方式　送信者Sは受信者Rに共通鍵で暗号化して送る

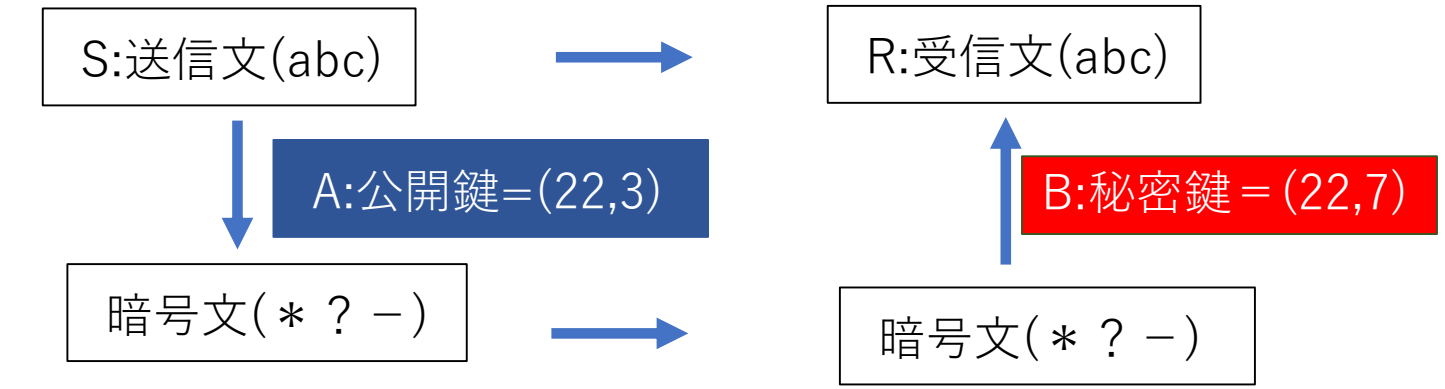


共通鍵は双方のみ知る秘密の鍵を使用

暗号鍵＝復号鍵

この場合は５　（５字ずらしの意味）

公開鍵方式　送信者Sは受信者Rの公開鍵で暗号化して送る



SはRの公開鍵Aで暗号化

Rは自分のみ知る秘密鍵Bで復号化

秘密鍵は公開鍵に依存し、簡単には見破れないものにする

暗号鍵 ≠ 復号鍵

例として、22=2×11
（実際には２つの非常に大きな素数を用いる）

公開鍵暗号方式

RSA暗号方式の仕組み

A:公開鍵=(n, r)

公開鍵 r ， 秘密鍵 s の作成手順
① n ＝ p×q
（p,qは大きな素数）
② L=LCM(p-1,q-1)
（LCM:最小公倍数）
③ r：GCM(r, L)=1 （1<r<L)
（GCM:最大公約数）
④ s：r×s ≡1 （mod L)
(1<s<L)

B:秘密鍵＝(n, s)

受信者：公開鍵A=（n, r)を作成

n ＝ p×q （p,qは大きな素数）
L=LCM(p-1,q-1)
r：Lと互いに素な整数

↓

送信者：送信文 a を公開鍵A=（n, r)で暗号化

$a^r \equiv b \pmod n$ を送信

↓

受信者：暗号文 b を秘密鍵 B=(n, s) で復号化

$b^s \equiv (a^r)^s \equiv a \pmod n$：復元

具体例

公開鍵A=（n, r)=(22, 3)を作成

n ＝ 22=2×11 （p=2, q=11）
L=10
r ＝ 3 （10と互いに素な整数）

↓

送信文 6 を公開鍵A=（22, 3)で暗号化

$6^3 \equiv 18 \pmod{22}$ を送信

↓

暗号文 18 を秘密鍵 B=(22, 7) で復号化

$18^7 \equiv (6^3)^7 \equiv 6 \pmod{22}$ 復元

・秘密鍵 s は p と q を用いた計算から作るが、その理論は数学的知識が必要となる（次のスライド）。

秘密鍵の数学的裏付けと作成方法

背景にある定理：p，q を素数とし，n＝p×q とする.このとき,
M= L×N＋1 （N=0, 1, 2, 3・・・自然数), ただし L＝LCM(p-1, q-1)
とすると, 自然数K（K＜N)に対して

$$K^M \equiv K \pmod{n}$$

が成立する.（オイラーの定理より）

例：p=2, q=11, n＝22 とする.このとき, M=（p－1とq－1の最小公倍数）×N＋1を21とすると,
例えば，K=4の時，$4^{21} \equiv 4 \pmod{22}$ となる.

秘密鍵の作成方法：(公開鍵：n，r）から （秘密鍵：n, s)を作る
p，q を素数とし,
n＝p×q ,
L＝LCM(p-1, q-1),
r ： Lと互いに素な整数とする(ie. GCM(r, L)=1).
そして，M= L×N＋1 （N=0,1,2,3・・・自然数)を考えて,
s ：r×s=M ≡1（mod L)
この s が秘密鍵になる.

例：p=2, q=11, n＝22 とする.このとき, M=（p－1とq－1の最小公倍数）×N＋1を21とすると,
例えば r =3とすることで， s＝21÷3＝7 となる.

秘密鍵の数学的裏付け（参考）

Fermatの小定理

p を素数とし，a と p は互いに素とするとき，

$a^{p-1} \equiv 1 \pmod{p}$

すなわち，a の p − 1 乗を p で割った余りは 1 である．

Eulerの定理

a を n と互いに素な整数とすると，

$a^{\phi(n)} \equiv 1 \pmod{n}$

が成り立つ．

ここで，$\phi(n)$ は n 未満の n と互いに素な自然数の個数を表し，オイラー関数 と呼ばれる．
特に n が素数のときは，$\phi(n) = n - 1$ より，フェルマーの小定理に一致する．

RSA暗号方式の演習問題

２つの素数p=11, q=13を用いてＲＳＡ暗号の公開鍵A：(n, r), 秘密鍵（n, s)を次の手順で作成せよ。

① N＝p×qを求めよ.

② L=LCM(p-1,q-1) を求めよ.

③ r を求めよ.（Lと互いに素な整数 ie GCM(r, L)=1 ）

④ r×s ≡1（mod L)をみたす s を求めよ.

⑤ 送信文 16 を公開鍵A=(n, r)で暗号化しよう.

⑥ 暗号文を秘密鍵 B=(n, s) で復号化 しよう.

公開鍵 r ， 秘密鍵 s の作成手順
① n ＝ p×q　　（p,qは大きな素数）

② L=LCM(p-1,q-1) or (p-1)(q-1)

③ r：GCM(r, L)=1

④ s：r×s ≡1（mod L)

解答例：
・公開鍵 A=(143, 7) , 秘密鍵 B=(143, 43)
・公開鍵 A=(143, 11) , 秘密鍵 B=(143, 11)

今後の課題

公開鍵の安全性は？
秘密鍵を生成している ｎ＝ｐ・ｑ が見破られない限り安全性，つまり素因数分解が鍵になるが，
これは，量子コンピュータなどの開発やリーマン予想の解決が影響する．

参考図書 ：
暗号の数理，一松信，ブルーバックス
暗号と情報社会，辻井重男，文春新書
インターネットセキュリティ，佐々木良一，岩波新書
１６歳のセアラが挑んだ世界最強の暗号，日本放送出版協会 （←おすすめ）

Mathematicaでのシミュレーション
http://www.f.waseda.jp/takezawa/math/joho/publickey/pub/index.html