

文系の、文系による、文系の為の 現代暗号基礎



-BaalzeBuB-



公開鍵暗号方式

- 電子署名
 - データの完全性を証明
- 鍵の認証
 - 鍵の保証、証明
- もちろん、暗号化
 - 秘匿性の確保
 - 実際の暗号化は？



電子署名

- どうやって本人の物だと証明する？
 - 対になっている2つの鍵の一方で暗号化されたデータは、それと対になるもう一つの鍵でのみ復号化出来る。

証明：花子さんの公開鍵で復号化出来たデータは花子さんの秘密鍵で暗号化されている。



鍵の認証

- 電子署名の問題

問題：ほな、その公開鍵をどうやって証明しよう？

解答：第三者(CA)に証明してもらおう

問題：その第三者(CA)をどうやって証明しよう？

解答：第四者(CA)に証明してもらおう

と、永遠に無限ループですな。ヽ(;´　`)ノ

実際には：メジャーなアプリケーションにはCAの証明書
がバンドルされている

でも、これって??



暗号化の秘密

- 公開鍵暗号方式のアルゴリズム

- 素因数分解の難解さが暗号の強さの秘密

- 解説： $71 * 97 = 6887$ は簡単でも

- $6887 = 71 * 97$ を求めるは難しいという事

- 実際には155桁ぐらいの数を使っている

- $A > C$ 、 $B > C$ のとき $A \div C$ と $B \div C$ の余りは同じになる事がある

- 解説： $10/4 = 2...2$ と $10/8 = 1...2$



さあ、皆でやってみよー

- 任意の素数を2つ選ぶ
ここでは17と19とする
- 選択した2つの素数から1引いた数の最小公倍数を求める

$$\text{Lcm}((17-1), (19-1))=144$$



鍵の生成

- 選択した素数の積を求める(公開鍵)
17*19=323となる
- 先に求めた最小公倍数よりも小さく、互いに素になる数を選ぶ(公開鍵)
ここでは139とする
- $139x \div 144 = y + 1$ の時、 y が最小の整数となる x を求める(秘密鍵)
 $x = 115$ となる



暗号化、複合化

- 暗号化

$$C = M^e \bmod N$$

解説： $M^e \div N = ? + C$ C は余りという意味

例： $122^{139} \div 323 = 3124 \dots 160$

- 複合化

$$M = C^d \bmod N$$

解説： $C^d \div N = ? + M$ M は余りという意味

例： $160^{115} \div 323 = 9217 \dots 122$



まとめ

- 簡単、かつ適当ですが
わかっていただけましたでしょうか？
- 私もいっぱいいっぱいです(笑)

いじよ。



蠅