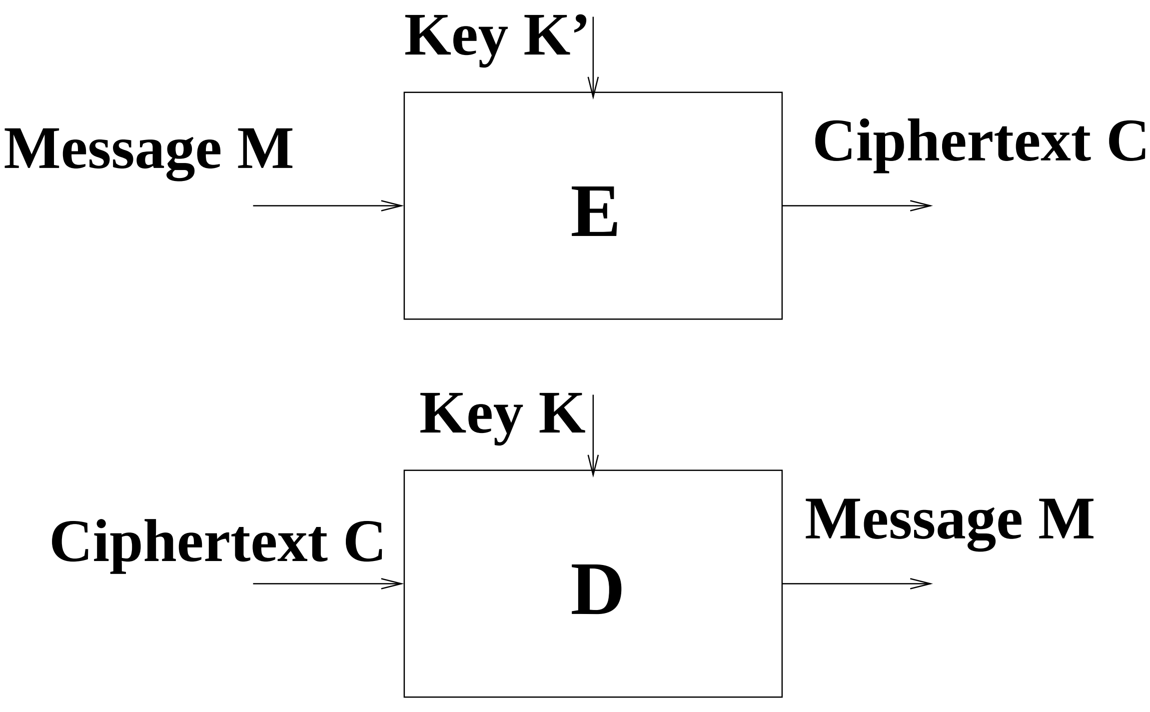
暗号入門7講の6
「暗号の攻撃手法」レジメ

松尾 和人

7月6日

現代暗号



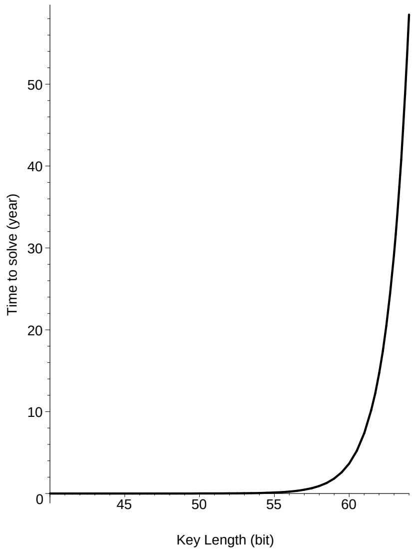
不特定多数の利用が前提 ⇒ E と D は公開

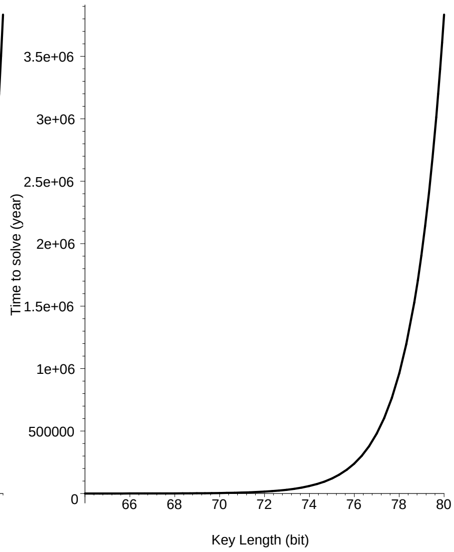
K の取り得る値は有限 ⇒ K を全部調べれば暗号は解ける

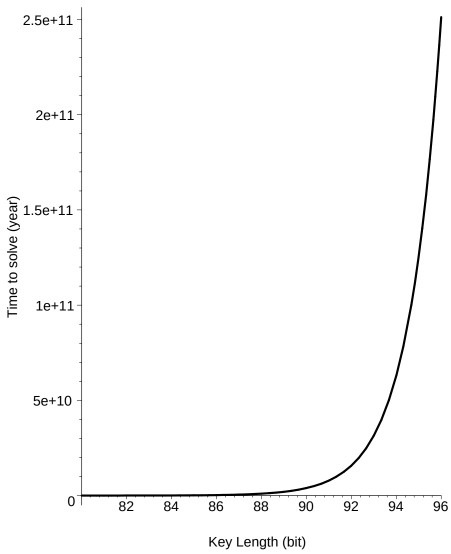
「安全」: ×解けない ⇒ ○解くのに時間がかかる

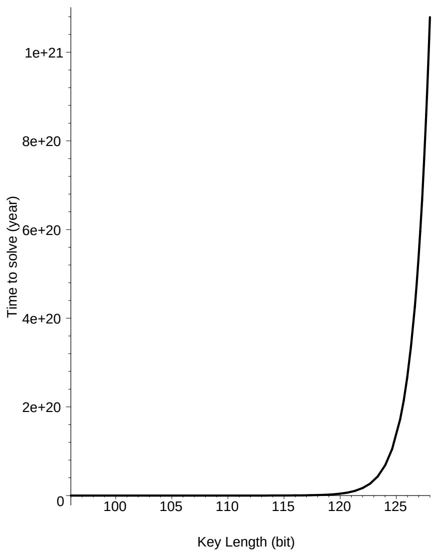
どれくらいの時間で解けるのか？

1 秒間に 10^{10} 個の鍵を調べられたとすると：









鍵長が 80-bit 程度で安全そうである。

鍵長が 128-bit 程度あれば、まず解けないであろう。

鍵長が 64-bit 程度あっても、用途によっては十分であろう。

現代暗号への攻撃

Known: E, D
Given: $\{(M, C)\}$
Find K.

- 既知暗号文攻撃：
  ランダムに与えられた $\{C\}$ を用いる。（通常無理）
- 既知平文攻撃：
  ランダムに与えられた $\{(M, C)\}$ を用いる。
- 選択平文攻撃：
  特殊な $\{M\}$ に対する $\{(M, C)\}$ を用いる。

共通鍵暗号では
全数探索より計算量の少ない解読法が存在しないアルゴリズムを
安全な暗号とする

RSA 暗号 (1977: Rivest, Shamir, Adleman)

	バ バ
鍵生成	p, q: 素数 $n = pq$ $e \in \mathbb{Z}/(p-1)(q-1)\mathbb{Z}, \gcd(e, (p-1)(q-1)) = 1$ $d \in \mathbb{Z}/(p-1)(q-1)\mathbb{Z},\ ed \equiv 1 \bmod (p-1)(q-1)$
鍵公開	(e, n) を公開
	アントニオ
暗号化	$C \equiv M^e \bmod n$
	バ バ
復号	$M_d \equiv C^d \bmod n$
	$M_d \equiv (M^e)^d \equiv M \bmod n$

以降の仮定：

1. RSA の暗復号時間：$\tilde{O}(1)$
2. p, q：32bit

サイコロを k 回振ったときの最大値

2 回振ったときの最大値

1 回目＼2 回目	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	2	3	4	5	6
3	3	3	3	4	5	6
4	4	4	4	4	5	6
5	5	5	5	5	5	6
6	6	6	6	6	6	6

最大値の期待値 $E = \frac{1}{36}\sum_{1\le i\le 6} i(i^2-(i-1)^2) \approx 4.47$

$$\begin{aligned}\sum_{1\le i\le 6} i(i^2-(i-1)^2) &= 1(1^2-0^2)+2(2^2-1^2)+3(3^2-2^2)+4(4^2-3^2)+5(5^2-4^2)+6(6^2-5^2)\\ &= (1-2)1^2+(2-3)2^2+(3-4)3^2+(4-5)4^2+(5-6)5^2+6^3\\ &= 6^3-\sum_{1\le i\le 5} i^2\end{aligned}$$

$$\begin{aligned}\sum_{1\le i\le 6} i(i^k-(i-1)^k) &= 1(1^k-0^k)+2(2^k-1^k)+3(3^k-2^k)+4(4^k-3^k)+5(5^k-4^k)+6(6^k-5^k)\\ &= (1-2)1^k+(2-3)2^k+(3-4)3^k+(4-5)4^k+(5-6)5^k+6^{k+1}\\ &= 6^{k+1}-\sum_{1\le i\le 5} i^k\end{aligned}$$

$$\begin{aligned}E &= \frac{1}{6^k}\left(6^{k+1}-\sum_{1\le i\le 5} i^k\right)\\ &= 6-\frac{1}{6^k}\sum_{1\le i\le 5} i^k\\ &\ge 6-\frac{1}{6^k}\left(6^{k+1}\left(\frac{1}{k+1}+\frac{1}{2\cdot 6}+\frac{k}{12\cdot 6^2}\right)\right)\\ &= 6\left(1-\left(\frac{1}{k+1}+\frac{1}{2\cdot 6}+\frac{k}{12\cdot 6^2}\right)\right)\end{aligned}$$

n 面サイコロ

$$\begin{aligned} E &= \frac{1}{n^k}\left(n^{k+1} - \sum_{1\le i\le n-1} i^k\right) \\ &= n\left(1 - \left(\frac{1}{k+1} + \frac{1}{2n} + \frac{k}{12n^2}\right)\right) \end{aligned}$$

$$n - m = n\left(\frac{1}{k+1} + \frac{1}{2n} + \frac{k}{12n^2}\right) = \frac{k^2 + (6n+1)k + 12n^2 + 6n}{12nk + 12n}$$

$k \approx \sqrt{n} \Rightarrow n - m \approx \sqrt{n}$

Fermat の小定理

p：素数、$a^{p-1} \equiv 1 \bmod p \ {}^{\forall}a \in [1, p-1]$

$$\begin{aligned} a^p &= (1 + (a-1))^p \\ &= \sum_{0\le i\le p} \binom{p}{i}(a-1)^i \\ &\equiv 1 + (a-1)^p \\ &\equiv 1 + (a-1) \\ &\equiv a \bmod p \\ & \quad \because \binom{p}{0} = \binom{p}{p} = 1,\ p\left|\binom{p}{i}\right. \ {}^{\forall}i \ne 0, p \end{aligned}$$

素数判定

n_c：素数 $\Rightarrow a^{n_c-1} \equiv 1 \bmod n_c \ {}^{\forall}a \in [1, n_c-1]$

$\Rightarrow$

$a^{2^s t} \equiv 1 \bmod n_c \Rightarrow a^{2^{s-1}t} \equiv \pm 1 \bmod n_c$ （ただし、$n_c - 1 = 2^s t$）

$a^{2^{s-1}t} \equiv 1 \bmod n_c \Rightarrow a^{2^{s-2}t} \equiv \pm 1 \bmod n_c$

$\vdots$

$a^{2t} \equiv 1 \bmod n_c \Rightarrow a^{t} \equiv \pm 1 \bmod n_c$

n_c：素数 $\Rightarrow a^t \equiv 1 \bmod n_c$ or ${}^{\exists}i$ s.t. $a \equiv -1 \bmod n_c \ {}^{\forall}a \in \mathbb{N}_{<n_c}$

$a^t \not\equiv 1 \bmod n_c$ and ${}^{\nexists}i$ s.t. $a^{2^i t} \equiv -1 \bmod n_c,\ 0 \le i \le s-1$

$\Rightarrow n_c$：合成数

そうでないとき、「素数」と思う。間違える確率 $< 1/4$

数十回繰り返せば十分 $\Rightarrow$ 計算量：定数 $\tilde{O}(1)$

素因数分解

$n_c \mapsto \prod p_i$

実際は

(n_0, n_1) s.t. $n_c = n_0 n_1$ を求める。

そして（素数判定をしながら）これを繰り返す。

一つの因子を見付けるのに必要な計算量

p: n_c の最小因子 $\le \sqrt{n_c}$

エラトステネスの篩	$\tilde{O}(p)$
Pollard の ρ 法	$\tilde{O}(p^{1/2})$
楕円曲線法	$\exp(\tilde{O}((\log p)^{1/2}))$
2 次篩	$\exp(\tilde{O}((\log n_c)^{1/2}))$
数体篩	$\exp(\tilde{O}((\log n_c)^{1/2}))$

素因数分解の方法

ある $n_d \in \mathbb{N}$ に対し

$$\gcd(n_d, n_c) = d \neq 1, n_c \ \Rightarrow \ d \text{ は } n_c \text{の非自明な因子}$$

repeat
  n_d を選ぶ
  $d = \gcd(n_d, n_c)$
until $d \neq 1, n_c$
return d

n_d をどのように選ぶか？

Birthday Paradox

$S : \mathrm{set}, n_0 = \#S$

r 個の中に 1 組も同じ値のペアがない確率:

$$\begin{aligned}
\prod_{i=1}^{r} \frac{n_0 - i + 1}{n_0} = \prod_{i=1}^{r} \left(1 - \frac{i-1}{n_0}\right) &< \prod_{i=1}^{r} \exp\left(-\frac{i-1}{n_0}\right) \quad \because 1 + x \leq e^x \\
&= \exp\left(\sum_{i=1}^{r} -\frac{i-1}{n_0}\right) = \exp\left(-\frac{r(r-1)}{2n_0}\right) \\
&\approx \exp\left(-\frac{r^2}{2n_0}\right)
\end{aligned}$$

$$r = \sqrt{2(\log 2)n_0} \Rightarrow \exp\left(-\frac{r^2}{2n_0}\right) = 0.5$$

$\Rightarrow O(\sqrt{n_0})$ 個の中には一致するペアがある確率が高い

Pollardのρ法

もし、$n_0 \mid n_c$ならば

$i = 1, \ldots, r$に対し、$a_i \in [0, n_c - 1]$を選択したとき

$r = O(\sqrt{n_0}) \Rightarrow a_i \equiv a_j \bmod n_0$ となる (a_i, a_j)が高確率で存在

（$n_0 = p$と考えてよい。ここでpはn_cの最小の素因子）

$n_d = a_i - a_j \equiv 0 \bmod n_0 \Rightarrow n_0 \mid \gcd(n_d, n_c)$,

多くの場合$\gcd(n_d, n_c) \neq n_c$

(a_i, a_j)をどのように探すか？

$a_{i+1} \equiv f(a_i) \bmod n_c$ とする。

$f(X)$：$\{a_1, a_2, \ldots\}$がランダムに見えるような関数をとる。

e.g. $f(X) = X^2 + 1$

すると

$i < j$に対し$a_i = a_j \ \Rightarrow \ a_{i+u} = a_{j+u} \ {}^\forall u \in \mathbb{N}$

$\Rightarrow$

${}^\forall v \geq i$, $a_v = a_{v+l} = a_{v+2l} = a_{v+3l} = \ldots$

但し、$l = j - i$

ここで

$v = \lceil i/l \rceil l$ （lの最小の倍数$> i$、$v \leq j = O(\sqrt{n_0}) = O(\sqrt{p})$）

$\Rightarrow$

$a_v = a_{v + \lceil i/l \rceil l} = a_{2v} \Rightarrow$ インデックスが2倍の値との比較のみでよい。

Rho 法の実際

```
a ∈ [0, n_c − 1], b = a
repeat
    a = f(a), b = f(f(b))
    d = gcd(a − b, n_c)
until d ≠ 1, n_c
return d
```

計算量

$\tilde{O}(\sqrt{p}) + \tilde{O}(\sqrt{p}) = \tilde{O}(\sqrt{p})$

中国の剰余定理

$$\begin{aligned} e_c &\equiv e_p \bmod p-1, \\ e_c &\equiv e_q \bmod q-1 \\ \Rightarrow & \\ e_c &\equiv e_p(q-1)y_p + e_q(p-1)y_q \bmod (p-1)(q-1), \\ & y_p \equiv 1/(q-1) \bmod p-1, y_q \equiv 1/(q-1) \bmod q-1 \end{aligned}$$

$e_p \bmod p-1$ を求める

離散対数問題：$(M_1, C_1) \mapsto e_c$ s.t. $C_1 \equiv M_1^{e_c} \bmod p$

Baby step giant step アルゴリズム (Shanks, Knuth)

任意の $1 \le b < p-1$ に対して

$^\exists(i, j)$ s.t. $e_c = jb + i$, $0 \le i < b$, $0 \le j < \lceil (p-1)/b \rceil$

そこで

$$C_1 M_1^{-jb} \equiv M_1^i \bmod p$$

を満足する (i, j) を探せばよい。

計算量：$b \approx \sqrt{p}$ のとき $\tilde{O}(\sqrt{p})$