乱数調整

原案: 矢藤

担当: 水野、矢藤

解説: 矢藤

問題

A, B, Xが与えられる。

- $a_0 = A$
- $a_{t+1} = (a_t / 2) \hat{} (a_t \% 2 * B)$

のとき、$a_t = X$ となる最小のtを求めよ。

解法

Baby-step giant-step algorithm

- 平方分割で離散対数問題を解くアルゴリズム
- 今回の問題は行列（or多項式）の離散対数問題
- 暗号学で有名

離散対数問題

$X = a^t \mod B$
となるような t を求める問題

離散対数問題への帰着

- 与えられた式: $a_{t+1} = (a_t / 2) \hat{} (a_t \% 2 * B)$
- a_t ,B をビットベクトルだと思えば
  - $a_{t,1} = a_{t,2} + a_{t,1} * B_1$
  - $a_{t,2} = a_{t,3} + a_{t,1} * B_2$
  - …
  - $a_{t,n-1} = a_{t,n} + a_{t,1} * B_{n-1}$
  - $a_{t,n} = a_{t,1} * B_n$

バイナリ行列Mを使って

- $a_{t+1} = M\ a_t \quad \Rightarrow \quad X = M^t\ A$

Baby-step giant-step algorithm

- a_t は周期性を持ち、長くても2^36
- H = 2^18 として、M^Hを計算

- MX, M^2X, ..., M^HXを計算 (1ごとのステップ)
- M^HA, $M^{2H}A$, ..., $M^{HH}A$を計算: (Hごとのステップ)

- どこかで$M^jX = M^{iH}A$となる！
- $X = M^{iH-j}A$?

Baby-step giant-step algorithm (つづき)

- $M^jX = M^{iH}A$ だからといって
  必ずしも $X = M^{iH-j}A$ とは限らない
- 例えば B = 0 のとき

- 計算量はO(sqrt(n) log n)

結果

- First Accept
  - hos.lyric* (173:44)
- Accepted/Submission
  - 6 / 90 (7%)