

CTF 入門

乱数の次の 値を予測する

@kurenaif



次でる値がわかる！

身の回りにある乱数

麻雀の次の牌

ゲームの次の出る敵キャラ・ダメージ

セッション ID

セッション ID



ルーレットの次出る値



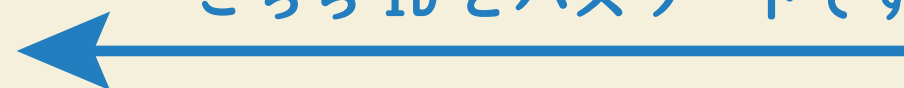
セッション ID とは？

セッション
ID の生成に
乱数を使う

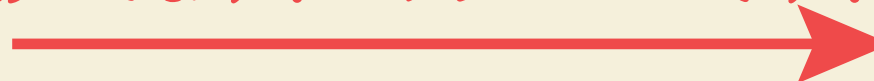


サーバー

こちら ID とパスワードです！



あってます！セッション ID です！



セッション ID です！

この機能を使いたいです！



そのセッション ID は Bob ですね！

OK です！



Bob

セッション ID が予測されると？



サーバー

セッション ID のやりとり

Marroly のセッション ID

セッション ID のやりとり

Bob のセッション ID

Bob のセッション ID はこれで

個人情報を教えてください

Bob ですね！個人情報です！

次の Bob のセッション ID はこれだな…



Marroly



Bob



Marroly

Bob の
個人情報
獲得

予測される乱数と予測されない乱数

予測される乱数（疑似乱数）

線形合同法

メルセンヌ・ツイスタ

XorShift

予測されない乱数

PC から出る熱雑音から生成された乱数（遅い）

→ /dev/random など

暗号論的疑似乱数生成器（CSPRNG）

→ 暗号やハッシュの技術を利用する

予測される乱数と予測されない乱数


予測される乱数（疑似乱数）

線形合同法

メルセンヌ・ツイスタ

XorShift

今日はこちらの
紹介



予測されない乱数

PC から出る熱雑音から生成された乱数（遅い）

→ /dev/random など

暗号論的疑似乱数生成器 (CSPRNG)

→ 暗号やハッシュの技術を利用する

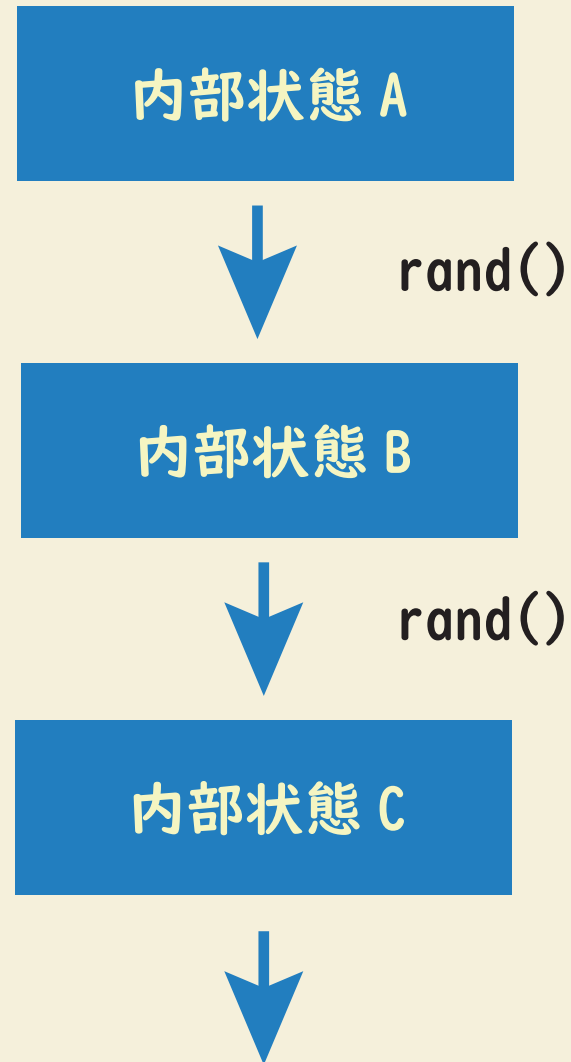
乱数を作る一般的な話

乱数を生成するときに引数を渡さない。
でも、次々違う値が出てくる

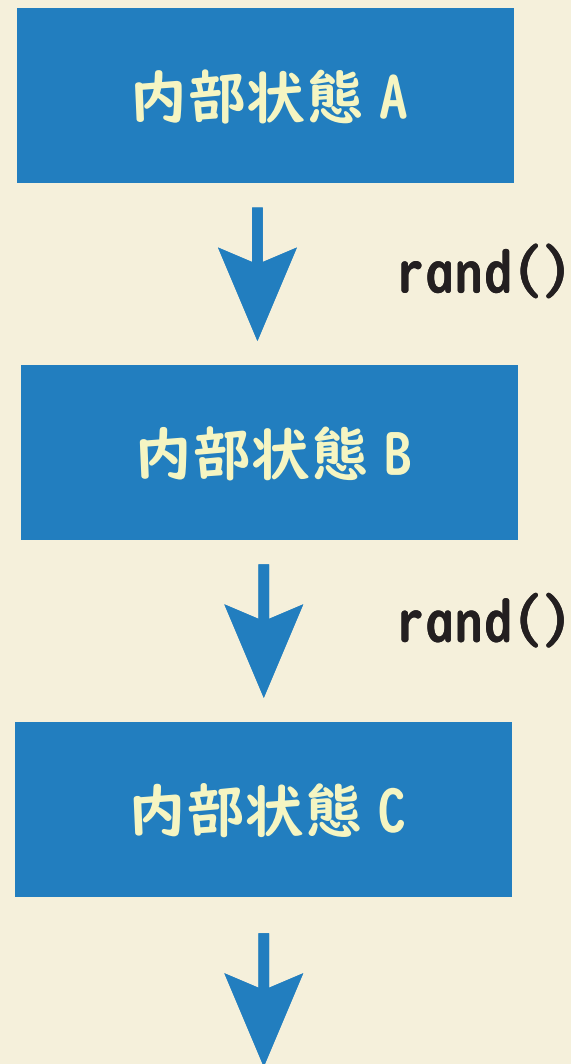
乱数は、**内部状態**を持っている

```
void solve() {  
    printf("%d", rand());  
}
```

乱数を作る一般的な話



乱数を作る一般的な話



内部状態と
rand のアルゴリズムと
乱数生成のパラメータ
がわかれば、次の
値がわかる。

乱数を作る一般的な話

初期パラメータは
seed 値
というもので決める
srand() など



内部状態 A



rand()

内部状態 B



rand()

内部状態 C



内部状態と

rand のアルゴリズムと
乱数生成のパラメータ
がわかれば、次の
値がわかる。

乱数生成アルゴリズム

rand のアルゴリズム

乱数生成のパラメータ

はソースコードに書いてある

```
protected synchronized int next(int bits)
{
    seed = (seed * 0x5DEECE66DL + 0xBL) & ((1L << 48) - 1);
    return (int) (seed >>> (48 - bits));
}
```

java.util.Random

内部状態と

rand のアルゴリズムと
乱数生成のパラメータ
がわかれば、次の
値がわかる。

→ 実装している言語 + 使用しているライブラリ +
内部状態で次の値を特定できる

線形合同法

次はここに入る

$$X_{n+1} = (A \times X_n + B) \mod M$$

$$A = 0x5DEECE66DL$$

$$B = 0xBL$$

$$M = 2^{48} - 1$$

```
protected synchronized int next(int bits)
{
    seed = (seed * 0x5DEECE66DL + 0xBL) & ((1L << 48) - 1);
    return (int) (seed >>> (48 - bits));
}
```

X は乱数の結果なので、得られる。(java の seed 相当)

(実際には java はここから加工されているので
工夫が必要)

今日の本題

$$X_{n+1} = (A \times X_n + B) \mod M$$

Q. A も B も M もわからないとき、
 X の値のみで、乱数予測はできるのか？

B だけわからないとき

note: X_0 は初期状態なので未知とする

$$X_1 = (A \times X_0 + B) \mod M$$

$$X_2 = (A \times X_1 + B) \mod M$$

$$B = X_2 - AX_1 \mod M$$

X_1, X_2 から X_3 を求めることができた。

$$X_3 = A \times X_2 + B \mod M$$

A も B もわからないとき

$$X_1 = (A \times X_0 + B) \mod M$$
$$X_2 = (A \times X_1 + B) \mod M \quad (1)$$

$$X_3 = (A \times X_2 + B) \mod M \quad (2)$$

(2) - (1) は

$$\underbrace{X_3 - X_2}_{Y_2 \text{ と置く}} = \underbrace{A(X_2 - X_1)}_{Y_1 \text{ と置く}} \mod M$$
$$Y_2 = A(Y_1) \mod M$$

$$A = Y_2(Y_1)^{-1} \mod M$$

Y^{-1} とは…？

$$A = Y_2(Y_1)^{-1} \mod M$$

を求めるために、 $(Y_1)^{-1}$ が必要

普通だったら、例えば 2 だったら $\frac{1}{2} = 0.5$

でも MOD の世界には、小数は存在しない。

Y^{-1} とは…？






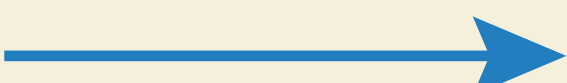
X^{-1} は、 X と掛け合わせたら 1 になるものを言う

逆行列も A^{-1} と表現する

$1/2$ も 2^{-1} と表現する

じゃあ MOD の世界で、かけ合わせたら 1 になる数は？

MOD7 の世界の X^{-1}

| | | |
|---|--|----------------------------------|
| 1 |  | $1 * 1 \bmod 7 = 1$ |
| 2 |  | $2 * 4 \bmod 7 = 8 \bmod 7 = 1$ |
| 3 |  | $3 * 5 \bmod 7 = 15 \bmod 7 = 1$ |
| 4 |  | $4 * 2 \bmod 7 = 8 \bmod 7 = 1$ |
| 5 |  | $5 * 3 \bmod 7 = 15 \bmod 7 = 1$ |
| 6 |  | $6 * 6 \bmod 7 = 36 \bmod 7 = 1$ |

これが X^{-1}

の正体！（全部バラバラ！）

M が素数のとき限定

どうやって求めるの？

$$Y Y^{-1} = 1 \pmod{M}$$

$$Y Y^{-1} = X M + 1$$

$$Y Y^{-1} - X M = 1 \quad (\text{ベズーの等式という})$$

Y と M が互いに素なとき、

ユークリッドの互除法を用いて

Y^{-1} と X を求めることができる！

Y と M が互いに疎なときのみ、求められる！

$$A = Y_2(Y_1)^{-1} \mod M$$

$$X_1 = (A \times X_0 + B) \mod M$$

$$X_2 = (A \times X_1 + B) \mod M$$

$$X_3 = (A \times X_2 + B) \mod M$$

A が既知になったので、あとは B を求めるだけ

A も B も M もわからないとき

6 つの値を使用する

$$X_1 = (A \times X_0 + B) \mod M \quad (1)$$

$$X_2 = (A \times X_1 + B) \mod M \quad (2)$$

$$X_3 = (A \times X_2 + B) \mod M \quad (3)$$

$$X_4 = (A \times X_3 + B) \mod M \quad (4)$$

$$X_5 = (A \times X_4 + B) \mod M \quad (5)$$

$$X_6 = (A \times X_5 + B) \mod M \quad (6)$$

A も M もわからないとき

さっきと同じ要領で引き算する

$$X_2 - X_1 = A(X_1 - X_0) \pmod{M} \quad (2) - (1)$$

$$X_3 - X_2 = A(X_2 - X_1) \pmod{M} \quad (3) - (2)$$

$$X_4 - X_3 = A(X_3 - X_2) \pmod{M} \quad (4) - (3)$$

$$X_5 - X_4 = A(X_4 - X_3) \pmod{M} \quad (5) - (4)$$

$$X_6 - X_5 = A(X_5 - X_4) \pmod{M} \quad (6) - (5)$$

A も M もわからないとき

さっきと同じ要領で変数に置く

$$Y_1 = A(Y_0) \mod M \quad (7)$$

$$Y_2 = A(Y_1) \mod M \quad (8)$$

$$Y_3 = A(Y_2) \mod M \quad (9)$$

$$Y_4 = A(Y_3) \mod M \quad (10)$$

$$Y_5 = A(Y_4) \mod M \quad (11)$$

A も M もわからないとき

少し計算してみる

$$Y_1 = A(Y_0) \mod M \quad (7)$$

$$Y_2 = A(Y_1) = A(A(Y_0)) = A^2 Y_0 \mod M \quad (8)$$

$$Y_3 = A(Y_2) = A(A^2 Y_0) = A^3 Y_0 \mod M \quad (9)$$

$$Y_4 = A(Y_3) = A(A^3 Y_0) = A^4 Y_0 \mod M \quad (10)$$

$$Y_5 = A(Y_4) = A(A^4 Y_0) = A^5 Y_0 \mod M \quad (11)$$

A も M もわからないとき

$$Y_1 = AY_0 \pmod{M} \quad (7)$$

$$Y_2 = A^2Y_0 \pmod{M} \quad (8)$$

$$Y_3 = A^3Y_0 \pmod{M} \quad (9)$$

$$Y_4 = A^4Y_0 \pmod{M} \quad (10)$$

$$Y_5 = A^5Y_0 \pmod{M} \quad (11)$$

さらに少し計算してみる

$$(7) \times (10) - (8) \times (9)$$

$$\underline{Y_1 \times Y_4 - Y_2 \times Y_3} = AY_0 \times A^4Y_0 - A^2Y_0 \times A^3Y_0$$

$$\begin{aligned} \text{Z1 と置く} &= A^5Y_0 - A^5Y_0 \\ &= 0 \pmod{M} \end{aligned}$$

$$(8) \times (11) - (9) \times (10)$$

$$\underline{Y_2 \times Y_5 - Y_3 \times Y_4} = 0 \pmod{M}$$

$$\text{Z2 と置く}$$

この左辺を求めるときは
剰余を求めないこと！！

M がわからないとき

$$Z_1 = 0 \pmod{M}$$

$$Z_2 = 0 \pmod{M}$$

つまり、何らかの I と J が存在して、

$$Z_1 = MI$$

$$Z_2 = MJ$$

Z_1 、 Z_2 、 I 、 J がわからない状態で、

M を抽出したい → 最大公約数を使う

M がわからないとき

$$Z_1 = MI$$

$$Z_2 = MJ$$

最大公約数： Z_1 と Z_2 を割り切る値。

両方とも **M** の倍数なので、**M** が必ず出てくる！

M がわかったら→A と B がわからないときの話になるので、解ける。

注：I と J の最大公約数が 1 でない場合、誤った値が出てきますが、その可能性は低いです。

Z の数を増やして 3 つの最大公約数を取れば、より安全になります。

今日のまとめ。

$$X_{n+1} = (A \times X_n + B) \mod M$$

X の値だけで A と B と M を求めることができた！

これで、内部状態、アルゴリズム、パラメータ
すべてわかるので、次の値を求めることができる

次回：実際にライブラリの乱数予測をする

問題 I

A も B も M も与えられます。
一つの X が与えられるので、
次の X を予測してください。

https://github.com/kurenaif/kurenaifCTF/tree/master/lcg_1

問題 2

A と M が与えられます。
2 つの X が与えられるので、
次の X を予測してください。

https://github.com/kurenaif/kurenaifCTF/tree/master/lcg_2

問題 3

M が与えられます。

3 つの X が与えられるので、
次の X を予測してください。

https://github.com/kurenaif/kurenaifCTF/tree/master/lcg_3

問題 4

6 つの X が与えられるので、
次の X を予測してください。

https://github.com/kurenaif/kurenaifCTF/tree/master/lcg_4