ANALISIS TEORITIS DAN EMPIRIS UJI CRAPS DARI *DIEHARD BATTERY OF RANDOMNESS TEST* UNTUK PENGUJIAN PEMBANGKIT BILANGAN ACAKSEMU

Sari Agustini Hafman[1] dan Arif Fachru Rozi[2]

[1,2] Lembaga Sandi Negara
e-mail: sari.hafman@lemsaneg.go.id[1], arif.fachru@lemsaneg.go.id[2]

ABSTRAK

Menurut Kerchoffs (1883), keamanan sistem kriptografi harus hanya bergantung pada kunci yang digunakan dalam sistem tersebut. Umumnya, kunci dihasilkan oleh *Pseudo Random Number Generator* (PRNG) atau *Random Number Generator* (RNG). Terdapat tiga tipe keacakan yang dihasilkan oleh PRNG dan RNG yaitu *pseudorandom sequence* (barisan acaksemu), *cryptographically secure pseudorandom sequences* (barisan acaksemu yang aman secara kriptografi) dan *real random sequences* (barisan yang acak nyata). Untuk memeriksa tipe keacakan yang dihasilkan oleh suatu PRNG atau RNG digunakan berbagai uji statistik, diantaranya *diehard battery of test of randomness*. Mengingat tujuan, dasar pengambilan parameter pengujian serta proses pembentukan statistik uji berhubungan dengan valid atau tidaknya kesimpulan yang dihasilkan dari suatu uji statistik maka dilakukan kajian terhadap salah satu uji yang terdapat dalam *diehard battery of randomness test* yaitu uji craps. Uji yang terinspirasi dari permainan craps ini bertujuan untuk memeriksa apakah suatu PRNG menghasilkan barisan acaksemu yang berdistribusi identik dan independen (iid). Untuk menunjukkan proses pembentukan serta penerapan permainan craps pada statistik uji craps, dilakukan analisis teoritis dengan menerapkan berbagai teori statistik terhadap uji tersebut. Selain itu, dilakukan observasi secara empiris dengan menerapkan uji craps pada beberapa PRNG dengan tujuan untuk memeriksa keefektifan uji tersebut dalam mendeteksi bentuk distribusi dan independensi barisan yang dihasilkan suatu PRNG.

Kata kunci: Identik dan Independen (iid), Permainan Craps, *Pseudo Random Number Generator* (PRNG), Uji Craps

ABSTRACT

According to Kerchoffs (1883), the security system should only rely on cryptographic keys which is used in that system. Generally, the key sequences are generated by a Pseudo Random Number Generator (PRNG) or Random Number Generator (RNG). There are three types of randomness sequences that generated by the RNG and PRNG i.e. pseudorandom sequence, cryptographically secure pseudorandom sequences, and real random sequences. Several statistical tests, including diehard battery of tests of randomness, is used to check the type of randomness sequences that generated by PRNG or RNG. Due to its purpose, the principle on taking the testing parameters and the test statistic are associated with the validity of the conclusion produced by a statistical test, then the theoretical analysis is performed by applying a variety of statistical theory to evaluate craps test, one of the test included in the diehard battery of randomness tests. Craps test, inspired by craps game, aims to examine whether a PRNG produces an independent and identically distributed (iid) pseudorandom sequences. To demonstrate the process to produce a test statistics equation and to show how craps games applied on that test, will be carried out theoretical analysis by applying a variety of statistical theory. Furthermore, empirical observations will be done by applying craps test on a PRNG in order to check the test effectiveness in detecting the distribution and independency of sequences which produced by PRNG.

Keywords: *Craps Games, Craps Test, Independent and Identically Distributed (iid), Pseudo Random Number Generator (PRNG)*

PENDAHULUAN

Menurut Kerchoffs (1883), keamanan sistem kriptografi harus hanya bergantung pada kunci yang digunakan dalam sistem tersebut. Umumnya, kunci dihasilkan oleh *Pseudo Random Number Generator* (PRNG) atau *Random Number Generator* (RNG). Terdapat tiga tipe keacakan yang dihasilkan oleh PRNG dan RNG yaitu *pseudorandom sequence* (barisan acaksemu), *cryptographically secure pseudorandom sequences* (barisan acaksemu yang aman secara kriptografi) dan *real random sequences* (barisan yang acak nyata). Barisan dikatakan acaksemu jika secara

statistik terlihat acak (berdistribusi seragam dan saling bebas). Barisan dikatakan aman secara kriptografis bila barisan tersebut secara statistik terlihat acak serta *unpredictable* (ketidak-terdugaan). Barisan dikatakan acak nyata bila memenuhi tiga syarat yaitu barisan tersebut secara statistik terlihat acak, ketidakterdugaan dan barisan yang sama tidak dapat dihasilkan kembali (Schneier, 1996).

Untuk memeriksa tipe keacakan yang dihasilkan oleh suatu PRNG atau RNG pendekatan yang umum digunakan adalah membangkitkan barisan kunci dalam jumlah besar dang mengaplikasikan berbagai uji statistik pada barisan tersebut. Uji statistik yang banyak digunakan diantaranya *diehard battery of test of randomness*. Informasi yang diperoleh dari hasil pengujian keacakan hanya untuk membedakan barisan kunci tersebut dari barisan kunci yang acak nyata. Uji tersebut dianggap sebagai uji yang menggunakan pendekatan *black box* karena tidak memperhitungkan struktur dari PRNG/RNG yang digunakan untuk menghasilkan barisan tersebut.

Mengingat tujuan, dasar pengambilan parameter pengujian serta proses pembentukan statistik uji berhubungan dengan valid atau tidaknya kesimpulan yang dihasilkan dari suatu uji statistik maka dilakukan kajian terhadap salah satu uji yang banyak digunakan dalam pengujian keacakan barisan kunci yaitu uji craps yang terdapat dalam *diehard battery of randomness*. Uji yang terinspirasi dari permainan craps ini bertujuan untuk memeriksa apakah suatu PRNG menghasilkan barisan acaksemu yang berdistribusi identik dan independen (iid) atau tidak.

Untuk menunjukkan proses pembentukan serta penerapan permainan craps pada statistik uji craps, dilakukan analisis teoritis dengan menerapkan berbagai teori statistik terhadap uji tersebut. Selain itu, dilakukan observasi secara empiris dengan menerapkan uji craps pada beberapa PRNG dengan tujuan untuk memeriksa keefektifan uji tersebut dalam mendeteksi bentuk distribusi dan independensi barisan yang dihasilkan suatu PRNG.

TEORI DASAR

Distribusi Normal

Distribusi Normal adalah model distribusi kontinu yang penting dalam teori probabilitas. Distribusi normal memiliki kurva berbentuk lonceng yang simetris. Dua parameter yang menentukan distribusi normal adalah *mean* (μ) dan variansi (σ^2). Fungsi kerapatan probabilitas dari distribusi normal adalah:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

μ adalah rata-rata, σ^2 adalah variansi dan $\pi = 3{,}14159\cdots$

Teorema 1 :

Jika X adalah suatu peubah acak binom dengan *mean* $\mu = np$ dan variansi $\sigma^2 = npq$ maka bentuk limit dari distibusi

$$Z = \frac{X - np}{\sqrt{npq}}$$

dengan $n \to \infty$ adalah berdistribusi $N(0,1)$.

Distribusi Chi-Square

Variabel acak kontinu X mempunyai distribusi *chi square* dengan derajat bebas *v* jika fungsi kerapatannya adalah

$$f(x;v) = \begin{cases} \frac{1}{2^{\frac{v}{2}}\Gamma\left(\frac{v}{2}\right)} x^{\frac{v}{2}-1} e^{-\frac{x}{2}} & , x > 0 \\ 0, \text{ lainnya} \end{cases}$$

dengan *v* adalah integer positif.

Distribusi Multinomial

Definisi 1. (Soejati,2005)

Distribusi multinomial adalah distribusi peluang bersama frekuensi-frekuensi sel $n_1, \cdots, n_k$ dalam n trial multinomial dengan parameter $p_1, \cdots, p_k$ yang masing-masing merupakan peluang sel.

Fungsi peluang distribusi multinomial adalah

$$f(n_1, \cdots, n_k) = \frac{n!}{n_1! \cdots n_k!} p_1^{n_1} \cdots p_k^{n_k}$$

untuk $\sum_{i=1}^{k} n_i = n$. Parameter-parameter itu memenuhi $\sum_{i=1}^{k} p_i = 1$

Nilai ekspektasi dan variansi dari distribusi multinomial adalah $E(n_i) = np_i$ dan $Var(n_i) = np_i(1 - p_i)$ dimana $i = 1{,}2, \cdots, k$.

Teorema 2.

Misalkan $y_1, \cdots, y_k$ berdistribusi multinomial dengan probabilitas $p_1, \cdots, p_k$ maka untuk *n* besar, variabel acak tidak negatif

$$\chi^2 = \sum_{i=1}^{k} \frac{(y_i - np_i)^2}{np_i} \text{ dimana } i = 1{,}2, \cdots, k \qquad (1)$$

mendekati distribusi *chi-square* dengan derajat bebas $= k - 1$ dengan harga *mean* χ^2 adalah $\mu = k - 1$.

Persamaan 1 pertama kali diperkenalkan dan dipelajari oleh Karl Pearson pada tahun 1900 sehingga dikenal dengan nama "*Pearson's chi square statistic*".

Harga *mean* χ^2 hanya tergantung pada banyak sel atau kelas k (banyak kemungkinan yang dapat terjadi pada eksperimen multinomial) dan tidak tergantung pada harga $p_i, i = 1,2,\cdots,k$.

Bukti :

$$mean(\chi^2) = E(\chi^2) = \sum_{i=1}^{k} \frac{E(y_i - np_i)^2}{np_i}$$
$$= \sum_{i=1}^{k} \frac{var(y_i)}{np_i} = \sum_{i=1}^{k} \frac{np_i(1-p_i)}{np_i}$$
$$\sum_{i=1}^{k} 1 - p_i = \sum_{i=1}^{k} 1 - \sum_{i=1}^{k} p_i = k - 1$$

Rumus transformasi χ^2 sering ditulis dengan persamaan

$$\chi^2 = \sum_{i=1}^{k} \frac{(y_i - np_i)^2}{np_i} = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$$

dengan $O_i = y_i$ adalah frekuensi sel i yang diobservasi dalam sampel berukuran n, sedangkan $E_i = np_i = mean(y_i)$ adalah *mean* atau frekuensi sel i yang diharapkan (nilai ekspektasi).

Uji Chi-Square Goodness of Fit

Teorema 3.

Uji *chi-Square goodness of fit* antara frekuensi yang diobservasi dengan frekuensi yang diharapkan, berdasarkan pada ukuran

$$\chi^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \qquad (2)$$

dengan χ^2 adalah nilai variabel acak yang distribusi samplingnya hampir mendekati distribusi *chi-square* dengan derajat bebas $v = k - 1, O_i$ adalah frekuensi yang diobservasi dan E_i adalah frekuensi yang diharapkan untuk setiap sel ke-*i*.

Prosedur uji *chi-square goodness of fit* berdasarkan atas distribusi pendekatan maka prosedur ini sebaiknya tidak digunakan jika frekuensi harapan sangat kecil atau $e_i < 5$. Jika dalam proses perhitungan terdapat frekuensi harapan yang lebih kecil dari lima maka frekuensi tersebut dapat digabungkan dengan frekuensi yang lain supaya prosedur diatas terpenuhi (Soejati, 1985).

Uji Craps

Ide uji craps berasal dari permainan craps. Craps merupakan suatu permainan yang melibatkan dua buah dadu yang dilakukan oleh seorang pemain atau lebih. Craps dimainkan dalam babak (round) yang diatur dalam aturan permainan craps. Berikut adalah aturan permainan Craps.

a. Jika jumlah mata dadu 7 atau 11 pada lemparan pertama maka pelempar dinyatakan menang.
b. Jika jumlahnya 2,3, atau 12 maka pelempar kalah.
c. jika jumlahnya 4,5,6,8,9 atau 10 maka pelempar dapat melanjutkan lemparannya sampai ia mendapatkan angka yang sama seperti lemparan pertama (dinyatakan menang) atau 7 (dinyatakan kalah).

Berdasarkan aturan permainan craps tersebut, Marsaglia mengajukan uji craps yang terdiri dari dua buah uji statistik yaitu :

a. uji untuk menganalisis jumlah kemenangan (uji 1)

   Pada uji ini diasumsikan permainan dilakukan sebanyak *n* kali, minimal 200.000 kali. Dari *n* kali permainan tersebut akan dihitung jumlah kemenangannya. Banyaknya kemenangan harus mendekati distribusi normal dengan rataan $200.000p$ dan variansi $200.000p(1\text{-}p)$ dengan $p = 244/495$.

b. uji untuk menganalisis banyaknya lemparan sampai permainan selesai (uji 2)

   Pada uji ini akan dihitung banyaknya melakukan lemparan dadu yang dilakukan seorang pemain sampai permainannya selesai. Banyaknya lemparan yang dilakukan oleh setiap pemain dapat bervariasi mulai dari 1 sampai tak hingga. Tetapi pada uji ini meskipun pemain dapat melakukan lemparan lebih dari 21 kali, lemparan tetap dianggap sebanyak 21 kali sehingga jumlah lemparan hanya akan dikelompokkan kedalam 21 kelas. Banyaknya lemparan harus berdistribusi chi-square dengan derajat bebas 20.

Pseudorandom Number Generator (PRNG)

Definisi 1 (Schneier, 1996):

PRNG adalah pembangkit barisan bilangan acaksemu, yang membutuhkan *seed* (input) dengan proses pembangkitan tiap elemen tergantung dari formulasi matematis yang digunakan pada PRNG tersebut.

Proses pembangkitan tiap elemen dari PRNG memiliki hubungan linier sesuai fungsi matematis yang digunakan, sehingga untuk meminimalisir kelinierannya, digunakan fungsi non-linier dan pengaturan parameter inputnya. Untuk memenuhi sifat *unpredictable*, pada umumnya PRNG menggunakan input berupa barisan bit acak yang berasal dari suatu RNG. Terdapat tiga tipe PRG berdasarkan prinsip kerjanya yaitu :

a. Tipe Linear

Tipe ini berdasarkan pada hubungan linear yang berulang yang digunakan untuk menghitung nilai selanjutnya dari nilai sebelumnya. Salah satu contoh PRNG bertipe Linear adalah *Multiply with Carry Generator* (MWC).

b. Tipe *Shift Register*

Tipe ini mengambil beberapa nilai yang berurutan dari suatu *multiple recursive generator* (MRG) untuk mengkonstruksi output selanjutnya. Contoh PRNG bertipe *shift register* adalah *shift register generator* 31 bit dan *shift register generator* 32 bit.

c. Tipe Nonlinear

Tipe PRNG yang tidak menghasilkan struktur berpola dan menghasilkan output yang berlaku seperti barisan yang acak nyata hampir di seluruh periode. Salah satu contoh PRNG bertipe nonlinear adalah *inverse congruential generator* (ICG).

METODE PENELITIAN

Penelitian ini terdiri atas dua tahap yaitu penelitian secara teoritis dan secara empiris. Berikut penjelasan dari kedua metode tersebut.

Penelitian Secara Teoritis

Penelitian secara teoritis dilakukan terhadap statistik uji craps baik uji 1 maupun uji 2 dengan menerapkan berbagai teori statistik terhadap uji-uji tersebut

Penelitian Secara Empiris

Data yang digunakan pada penelitian ini merupakan data simulasi yang berasal dari 10 PRNG yang berasal dari tiga tipe PRNG. Kesepuluh PRNG beserta parameternya seperti yang diperlihatkan pada Tabel 1. Jumlah data yang dibangkitkan oleh kesepuluh PRNG tersebut sebesar 11 Mbyte (Marsaglia,1985).

Tabel1. Sepuluh PRNG dan Parameternya

Tipe	Nama PRNG		Parameter
Linear	*Multiply With Carry* (MWC)	MWC-1	a=1791398085 x = 191, c = 17
		MWC-2	a=1447497129 x=191, c=17
		MWC-3	a=2083801278 x=191, c=17
Shift Register	*Shift Register Generator* (SRG) 31 Bit	SRG31-1	L=13, R=18
		SRG31-2	L=18, R=3
		SRG31-3	L=24, R=7
	Shift Register Generator (SRG) 32 Bit	SRG32-1	*Shift Register* 17 dan 15
		SRG32-2	*Shift Register* 15 dan 17
		SRG32-3	*Shift Register* 13, 17 dan 5
Nonlinear	*Inverse Congruential Generator* (ICG)		a = 9 b = 13 *seed* = 247

Karena uji *craps* bertujuan untuk menguji sifat keacakan dari suatu PRNG maka sebelum menerapkan uji craps terlebih dahulu dilakukan pembangkitan barisan kunci sebesar 11 Megabyte dari ketiga PRNG tersebut. Kedua statistik uji craps digunakan untuk menghitung *p-value*. *P-value* ini selanjutnya akan dibandingkan dengan tingkat kepercayaan (α). Tingkat kepercayaan yang digunakan dalam penelitian ini adalah 0,001. Jika $p - value \geq \alpha$ maka hipotesis nol diterima atau barisan dikatakan acak. Jika $p - value < \alpha$ maka hipotesis nol ditolak atau barisan dikatakan tidak acak.

PEMBAHASAN

Analisis Teoritis

Pada tahap ini dilakukan analisis teoritis dengan menerapkan berbagai teori statistik terhadap proses pembentukan statistik uji pada kedua statistik uji yang terdapat dalam uji craps. Hasil analisisnya adalah sebagai berikut.

a. Proses pembentukan statistik uji pada uji 1

Misalkan :

G adalah jumlah permainan, N adalah banyaknya lemparan, X_i, Y_i adalah outcome pada lemparan ke-i, $Z_i = X_i + Y_i$ adalah jumlah score pada lemparan ke-i, I adalah indikator ketika menang yang dinyatakan dengan :

$$I = \begin{cases} 1, \text{jika menang} \\ 0, \text{ jika kalah} \end{cases}$$

A adalah kejadian mendapat mata dadu berjumlah 7 atau 11

B adalah kejadian mendapat mata dadu berjumlah 4 pada lemparan ke-1 dan ke-2
C adalah kejadian mendapat mata dadu berjumlah 5 pada lemparan ke-1 dan ke-2
D adalah kejadian mendapat mata dadu berjumlah 6 pada lemparan ke-1 dan ke-2
E adalah kejadian mendapat mata dadu berjumlah 8 pada lemparan ke-1 dan ke-2
F adalah kejadian mendapat mata dadu berjumlah 9 pada lemparan ke-1 dan ke-2
G adalah kejadian mendapat mata dadu berjumlah 10 pada lemparan ke-1 dan ke-2
Probabilitas memperoleh mata dadu berjumlah 2,3,4,..., 12 pada lemparan pertama diperoleh sebagai berikut :

$$P(Z_1 = 2) = P(Z_1 = 12) = \frac{1}{36}$$
$$P(Z_1 = 3) = P(Z_1 = 11) = \frac{2}{36}$$
$$P(Z_1 = 4) = P(Z_1 = 10) = \frac{3}{36}$$
$$P(Z_1 = 5) = P(Z_1 = 9) = \frac{4}{36}$$
$$P(Z_1 = 6) = P(Z_1 = 8) = \frac{5}{36}$$
$$P(Z_1 = 7) = \tfrac{6}{36} \qquad (3)$$

Probabilitas jumlah kemenangan pada permainan craps diperoleh dari :

1) probabilitas memperoleh mata dadu bernilai 7 atau 11 pada lemparan pertama dari dua dadu
$$P(A) = P(Z_1 = 7) + P(Z_1 = 11) = \frac{2}{9}$$
2) probabilitas memperoleh mata dadu bernilai sama (4,5,6,8,9 atau 10) baik pada lemparan pertama atau kedua
$$P(B) = P(Z_1 = 4) \cdot P(I = 1|Z_1 = 4)$$
$$= P(Z_1 = 4) \cdot \frac{P(Z_1 = 4)}{P(Z_1 = 4) + P(Z_1 = 7)}$$
$$= \frac{3}{36} \cdot \frac{\frac{3}{36}}{\frac{3}{36} + \frac{6}{36}} = \frac{1}{36}$$
$$P(C) = P(Z_1 = 5) \cdot P(I = 1|Z_1 = 5)$$
$$= \frac{4}{36} \cdot \frac{4}{10} = \frac{2}{45}$$
$$P(D) = P(Z_1 = 6) \cdot P(I = 1|Z_1 = 6)$$
$$= \frac{5}{36} \cdot \frac{5}{11} = \frac{25}{396}$$
$$P(E) = P(Z_1 = 8) \cdot P(I = 1|Z_1 = 8)$$
$$= \frac{5}{36} \cdot \frac{5}{8} = \frac{25}{396}$$
$$P(F) = P(Z_1 = 9) \cdot P(I = 1|Z_1 = 9)$$
$$= \frac{4}{36} \cdot \frac{4}{10} = \frac{2}{45}$$
$$P(G) = P(Z_1 = 10) \cdot P(I = 1|Z_1 = 10)$$
$$= \frac{3}{36} \cdot \frac{3}{9} = \frac{1}{36}$$
$$P(I = 1) = \frac{2}{9} + 2 \cdot \frac{1}{36} + 2 \cdot \frac{2}{45} + 2 \cdot \frac{25}{396}$$
$$= \frac{244}{495}$$

sehingga $P(I = 0) = \frac{251}{495}$.
Karena jumlah kemenangan saat permainan craps diulang sebanyak 200.000 atau G = 200000 merupakan peubah acak binom dengan $p = \frac{244}{495}$ maka diperoleh

$$\mu = 200000 \cdot \frac{244}{495} = 98585{,}86$$
$$\sigma^2 = 200000 \cdot \tfrac{244}{495} \cdot \tfrac{251}{495}.$$

Dengan menggunakan teorema 1 diperoleh statistik uji pada uji 1 yaitu

$$zscore = \frac{X - np}{\sqrt{npq}} = \frac{X - 98585{,}86}{\sqrt{200000 \cdot \frac{244}{495} \cdot \frac{251}{495}}}.$$

Berdasarkan *central limit theorem*, untuk $n \to \infty$ distribusi dari $zscore = \frac{X - 98585{,}86}{\sqrt{200000 \cdot \frac{244}{495} \cdot \frac{251}{495}}}$ mendekati $N(0,1)$

b. Proses pembentukan statistik uji pada uji 2

Pada proses pembentukan statistik uji pada uji 2, terlebih dahulu harus dihitung probabilitas dari jumlah lemparan yang mungkin dilakukan seorang pemain. Seperti yang telah dijelaskan sebelumnya jumlah lemparan dikelompokkan kedalam 21 kelas mulai dari kelas 1 yang merepresentasikan pemain hanya dapat melakukan lemparan sebanyak satu kali atau dengan kata lain kalah pada lemparan pertama atau menang pada lemparan pertama. Dikatakan kalah pada lemparan pertama yaitu ketika jumlah mata dadu pada lemparan pertama bernilai 2, 3 atau 12, sedangkan dikatakan menang pada lemparan pertama adalah ketika mata dadu bernilai 7 atau 11. Kelas yang lain yaitu kelas 2 sampai 21 terjadi ketika jumlah mata dadu bernilai sama (4,5,6,8,9 atau 10) pada lemparan pertama, kedua dan seterusnya.

Berikut adalah proses pembentukan statistik ujinya.

1) Untuk kelas 1 ($N = 1$)
Karena probabilitas melempar hanya 1 kali adalah
$$P(N = 1|Z = z) = 1.$$
maka probabilitas kelas 1 adalah
$$P(N = 1) = P(Z = 2) \cdot P(N = 1|Z = 2)$$
$$+P(Z = 3) \cdot P(N = 1|Z = 3)$$
$$+P(Z = 12) \cdot P(N = 1|Z = 12)$$
$$+P(Z = 7) \cdot P(N = 1|Z = 7)$$
$$+P(Z = 11) \cdot P(N = 1|Z = 11)$$
$$= {}^{1}/_{36} \cdot 1 + {}^{2}/_{36} \cdot 1 + {}^{1}/_{36} \cdot 1$$

$$+{}^{6}/_{36}\cdot 1+{}^{2}/_{36}\cdot 1={}^{12}/_{36}$$

Setelah probabilitas dari kelas ke-1 diperoleh maka dapat dihitung nilai harapannya ketika G = 200000 yaitu

$$E(N=1)=200000\cdot P(N=1)$$
$$=200000\cdot {}^{12}/_{36}$$
$$=66666{,}7$$

2) Untuk kelas yang lain $(N=n)$ dengan $n=2,3,\cdots,20$

Probabilitas melempar sebanyak n kali merupakan distrisbusi geometri sehingga

$$P(N=n|Z=z)=P_{Z=z}\cdot(1-P_{Z=z})^{(n-1)-1}$$
$$=P_{Z=z}\cdot(1-P_{Z=z})^{n-2}$$

untuk $n=2,3,\cdots,20$ dengan $P_{Z=z}$ adalah probabilitas permainan berakhir saat muncul jumlah mata dadu $7(Z=7)$ yang pertama.

Sehingga

$$P_{Z=z}=P(Z=z)+P(Z=7).$$

maka untuk $z=4,5,6,8,9,10$ diperoleh

$$P_{Z=4}=P(Z=4)+P(Z=7)$$
$$={}^{3}/_{36}+{}^{6}/_{36}={}^{9}/_{36}$$
$$P_{Z=5}=P(Z=5)+P(Z=7)$$
$$={}^{4}/_{36}+{}^{6}/_{36}={}^{10}/_{36}$$
$$P_{Z=6}=P(Z=6)+P(Z=7)$$
$$={}^{5}/_{36}+{}^{6}/_{36}={}^{11}/_{36}$$
$$P_{Z=8}=P(Z=8)+P(Z=7)$$
$$={}^{5}/_{36}+{}^{6}/_{36}={}^{11}/_{36}$$
$$P_{Z=9}=P(Z=9)+P(Z=7)$$
$$={}^{4}/_{36}+{}^{6}/_{36}={}^{10}/_{36}$$
$$P_{Z=10}=P(Z=10)+P(Z=7)$$
$$={}^{3}/_{36}+{}^{6}/_{36}={}^{9}/_{36}$$

Probabilitas kelas ke-n adalah

$$P(N=n)=P(Z=4)\cdot P(N=n|Z=2)$$
$$+P(Z=5)\cdot P(N=n|Z=5)$$
$$+P(Z=6)\cdot P(N=n|Z=6)$$
$$+P(Z=8)\cdot P(N=n|Z=8)$$
$$+P(Z=9)\cdot P(N=n|Z=9)$$
$$+P(Z=10)\cdot P(N=n|Z=10)$$

karena $P(Z=4)=P(Z=10)$dan $P(N=n|Z=4)=P(N=n|Z=10)$ serta $P(Z=5)=P(Z=9)$dan $P(N=n|Z=5)=P(N=n|Z=9)$, maka

$$P(N=n)=2\cdot P(Z=4)$$
$$\cdot P(N=n|Z=4)+2\cdot P(Z=5)$$
$$\cdot P(N=n|Z=5)+2\cdot P(Z=6)$$
$$\cdot P(N=n|Z=6)$$
$$=2\cdot P(Z=4)\cdot P_{Z=4}(1-P_{Z=4})^{n-2}$$
$$+2\cdot P(Z=5)\cdot P_{Z=5}(1-P_{Z=4})^{n-2}$$
$$+2\cdot P(Z=6)\cdot P_{Z=6}(1-P_{Z=4})^{n-2}$$
$$=2\cdot {}^{3}/_{36}\cdot {}^{9}/_{36}\cdot\left(1-{}^{9}/_{36}\right)^{n-2}$$
$$+2\cdot {}^{4}/_{36}\cdot {}^{10}/_{36}\cdot\left(1-{}^{10}/_{36}\right)^{n-2}$$
$$+2\cdot {}^{5}/_{36}\cdot {}^{11}/_{36}\cdot\left(1-{}^{11}/_{36}\right)^{n-2}$$
$$={}^{1}/_{24}\left({}^{3}/_{4}\right)^{n-2}+{}^{5}/_{81}\left({}^{13}/_{18}\right)^{n-2}$$
$$+{}^{55}/_{648}\left({}^{25}/_{36}\right)^{n-2}$$

untuk $n=2,3,4,\cdots,20$

Tabel 2 Probabilitas dan Nilai Harapan dari Kelas ke-2 s.d. Kelas ke-20

Kelas ke-n	Probabilitas $P(N{=}n)$	Nilai Harapan $E(N{=}n)$
2	0,188271605	37654,3
3	0,134773663	26954,7
4	0,096567311	19313,5
5	0,0692571	13851,4
6	0,049717715	9943,5
7	0,035725128	7145,0
8	0,025695361	5139,1
9	0,018499325	3699,9
10	0,013331487	2666,3
11	0,009616645	1923,3
12	0,006943702	1388,7
13	0,005018575	1003,7
14	0,003630703	726,1
15	0,002629179	525,8
16	0,001905753	381,2
17	0,001382697	276,5
18	0,001004149	200,8
19	0,000729922	146,0
20	0,000531076	106,2

Seperti pada kelas ke-1 maka setelah diperoleh probabilitas dari masing-masing kelas maka dapat dihitung nilai harapannya ketika G = 200000 yaitu

$$E(N=n)=200000\cdot P(N=n)$$

untuk $n=2,3,4,\cdots,20$.

Probabilitas dan nilai harapan dari kelas ke-2 s.d. ke-20 ditampilkan pada Tabel 2.

3) Untuk kelas ke-21 (N = 21)

Pada uji 2 diasumsikan lemparan di atas 21 kali memiliki kemungkinan yang kecil untuk terjadi (seperti yang ditunjukkan pada Tabel 3) maka meskipun pemain dapat melakukan lemparan lebih dari 21 kali, lemparan tersebut dimasukkan dalam kelas ke-21. Akibatnya probabilitas kelas ke-21 merupakan gabungan dari probabilitas ketika lemparan mencapai 21 ditambah probabilitas ketika lemparan diatas 21 kali atau dapat dihitung sebagai berikut :

$$P(N=21)=1-[P(N=1)+P(N=2)$$
$$+\cdots++P(N=20)]=0{,}001436$$

sehingga nilai harapan kelas ke-21 ketika G = 200000 yaitu

$$E(N = 21) = 200000 \cdot 0{,}001436 = 287{,}1$$

Tabel 3 Probabilitas
Kelas ke-21 s.d. Kelas ke-35

Kelas ke-n	Probabilitas $P(N{=}n)$
21	0,000387
22	0,000282
23	0,000206
24	0,00015
25	0,00011
26	8,03E-05
27	5,88E-05
28	4,31E-05
29	3,16E-05
30	2,32E-05
31	1,7E-05
32	1,25E-05
33	9,19E-06
34	6,77E-06
35	4,98E-06

Karena banyaknya lemparan merupakan data berskala nominal dan tujuan dari uji adalah untuk mengetahui apakah banyaknya lemparan membentuk distribusi seperti yang diharapkan untuk suatu barisan acak maka staistik uji yang digunakan adalah *chi-square goodness of fit* yang dinyatakan dengan persamaan :

$$chisq = \sum_{n=1}^{21} \frac{\left(O_n - E(N = n)\right)^2}{E(N = n)}$$

dengan derajat bebas 20.

Berdasarkan prosedur uji *chi-square goodness of fit* yaitu nilai frekuensi harapan tiap kelas $e_i \geq 5$ maka pada uji 2 jumlah permainan yang harus dilakukan minimal harus lebih dari atau sama dengan 9415 kali atau $G \geq 9415$. Karena probabilitas kelas bervariasi maka nilai yang diambil sebagai rujukan adalah probabilitas terkecil. Dari kelas ke-1 s.d. kelas ke-21 probabilitas terkecil dimiliki oleh kelas ke-20 yaitu 0,000531076.

Bukti :

$e_i = G \cdot P(N = n)$ dengan minimal $P(N = 21) = 0{,}000531076$ maka $5 = G \cdot 0{,}000531076$ sehingga minimal $G = \frac{5}{0{,}000531076} = 9414{,}8485 = 9415$.

p adalah notasi untuk proporsi.

Basic step : $p(9415)$ benar karena $9415 \cdot 0{,}000531076 = 5{,}00008054 \geq 5$

Inductive step :

misalkan $p(G)$ benar sehingga $G \cdot 0{,}000531076 \geq 5$ maka akan ditunjukkan bahwa saat $p(G + 1)$ juga benar.

$$p(G + 1): (G + 1) \cdot 0{,}000531076 \geq 5 \Rightarrow$$
$$(G + 1) \cdot 0{,}000531076 = (G \cdot 0{,}000531076) + (0{,}000531076) \geq 5$$

Menurut hipotesis induksi $G \cdot 0{,}000531076 \geq 5$ sedangkan untuk $G > 9415$, nilai 0,000531076 lebih besar dari 0 sehingga 0,000531076 akan memperbesar nilai di ruas kanan persamaan. Akibatnya $(G \cdot 0{,}000531076) + (0{,}000531076) \geq 5$ jelas benar. Jadi G pada uji 2 adalah $G \geq 9415$. Pada uji 2 ini, Marsaglia merekomendasikan menggunakan G yang lebih besar dari 9415 yaitu 200000 (Marsaglia and Tsang, 2002).

Analisis Empiris

Hasil pengujian dengan menggunakan dua uji dari uji craps pada sepuluh PRNG ditampilkan baik dalam bentuk tabel maupun gambar. Tabel 4 memperlihatkan hasil pengujian dengan menggunakan uji craps ke-1 pada sepuluh PRNG.

Tabel 4. Hasil Pengujian dengan Menggunakan Uji Craps ke-1

Generator	Uji 1		
	z-score	P-value	Ket.
MWC-1	-3,269	0,00054	tdk acak
MWC-2	-0,053	0,47885	acak
MWC-3	-0,63	0,26435	acak
SRG31-1	-0,831	0,20291	acak
SRG31-2	2,152	0,98430	acak
SRG31-3	-0,178	0,42925	acak
SRG32-1	0,269	0,60603	acak
SRG32-1	-0,286	0,38759	acak
SRG32-3	0,269	0,60603	acak
ICG	0,73	0,76720	acak

Pada Tabel 4 terlihat bahwa hanya PRNG MWC-1 yang tidak lulus uji craps ke-1 sedangkan kesembilan PRNG yang lain lulus uji tersebut. Hal ini karena jumlah kemenangan sebenarnya (hasil observasi) MWC-1 memiliki nilai yang jauh lebih kecil dari jumlah kemenangan harapan dengan selisih sebesar 730,86. Berbeda dengan kesembilan PRNG lain yang memiliki selisih tidak terlalu jauh dari nilai harapan yaitu -185,86 s.d. 481,14. Informasi mengenai jumlah kemenangan observasi dan jumlah harapan kesepuluh PRNG tersebut ditampilkan pada Tabel 5. Berdasarkan informasi yang diperoleh dari Tabel 4 dan Tabel 5 terlihat bahwa uji craps ke-1 cukup efektif untuk

mendeteksi bentuk distribusi dan independensi barisan yang dihasilkan suatu PRNG.

Tabel 5 Jumlah Kemenangan vs Jumlah Harapan dari Sepuluh PRNG

Nama PRNG	Jumlah Menang		Selisih
	Observasi	Harapan	
MWC-1	97855	98585,86	-730,86
MWC-2	98574	98585,86	-11,86
MWC-3	98445	98585,86	-140,86
SRG31-1	98400	98585,86	-185,86
SRG31-2	99067	98585,86	481,14
SRG31-3	98546	98585,86	-39,86
SRG32-1	98646	98585,86	60,14
SRG32-2	98522	98585,86	-63,86
SRG32-3	98646	98585,86	60,14

Hasil pengujian pada kesepuluh PRNG dengan menggunakan uji craps ke-2 diperlihatkan pada Tabel 6. Pada Tabel 6 terlihat bahwa seluruh PRNG lulus uji ke-2. Hal ini karena nilai observasi pada tiap kelas tidak berbeda jauh dengan nilai harapannya. Sebagai contoh ditampilkan hasil pengujian dengan menggunakan uji craps ke-2 pada PRNG MWC-1 secara lengkap pada Tabel 7.

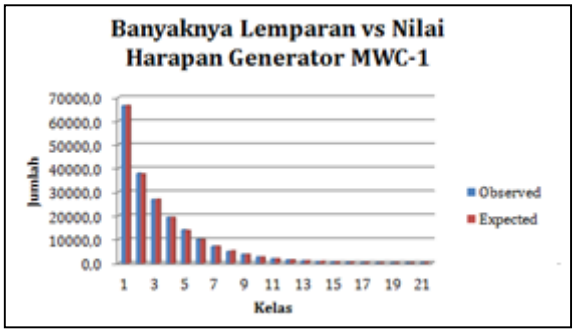
Tabel 6 Hasil Pengujian dengan Menggunakan Uji Craps ke-2

Generator	Uji 2 chisq	P-value	Ket.
MWC-1	26,69	0,855698	acak
MWC-2	22,55	0,688596	acak
MWC-3	19,82	0,530605	acak
SRG31-1	15,48	0,251595	acak
SRG31-2	18,4	0,438732	acak
SRG31-3	26,39	0,846570	acak
SRG32-1	16,33	0,303937	acak
SRG32-1	16	0,283332	acak
SRG32-3	16,33	0,303937	acak
ICG	19	0,478151	acak

Pada Tabel 7 terlihat bahwa nilai observasi pada tiap kelas tidak berbeda jauh dengan nilai yang diharapkan yaitu antara -205,1 s.d. 259,7. Hal tersebut diperkuat dengan Gambar 1. Pada Gambar 1 terlihat bahwa banyaknya lemparan sebenarnya (hasil observasi) dengan nilai harapan tiap kelas tidak memiliki selisih yang terlalu jauh.

Tabel 7 Hasil Pengujian dengan Menggunakan Uji Craps ke-2 pada MWC *Generator*-1

Kelas	Observed	Expected	Chisq	Sum
1	66490	66666.7	.468	.468
2	37914	37654.3	1.791	2.259
3	26889	26954.7	.160	2.419
4	19320	19313.5	.002	2.421
5	14088	13851.4	4.041	6.462
6	10026	9943.5	.684	7.146
7	7105	7145.0	.224	7.370
8	4934	5139.1	8.183	15.554
9	3713	3699.9	.047	15.600
10	2646	2666.3	.155	15.755
11	1904	1923.3	.194	15.949
12	1426	1388.7	1.000	16.949
13	978	1003.7	.659	17.607
14	670	726.1	4.340	21.948
15	512	525.8	.364	22.312
16	383	381.2	.009	22.321
17	268	276.5	.264	22.585
18	195	200.8	.169	22.754
19	160	146.0	1.346	24.099
20	115	106.2	.727	24.826
21	264	287.1	1.861	26.687



Gambar 1 Grafik Banyaknya Lemparan vs Nilai Harapan Tiap Kelas pada MWC-1

Berdasarkan informasi dari Tabel 6 dan Tabel 7 serta Gambar 1, terlihat bahwa uji craps ke-2 cukup efektif untuk mendeteksi bentuk distribusi dan independensi barisan yang dihasilkan suatu PRNG.

PENUTUP

Berdasarkan hasil penelitian yang telah dilakukan maka dapat disimpulkan bahwa :

1. Pada uji craps ke-1, jumlah kemenangan saat permainan craps merupakan peubah acak binom sehingga dengan menggunakan *central limit theorem* diperoleh bahwa statistik uji ke-1 mendekati distribusi normal baku.
2. Statistik uji yang digunakan pada uji craps ke-2 adalah uji *chi-square goodness of fit* dengan distribusi hipotesis adalah distribusi

multinomial karena banyaknya lemparan yang dihitung pada uji craps ke-2 merupakan data berskala nominal yang terdiri dari 21 kelas dan tujuan dari uji ke-2 adalah untuk mengetahui apakah banyaknya lemparan membentuk distribusi seperti yang diharapkan untuk suatu barisan acak.

3. Sesuai dengan prosedur uji *chi-square goodness of fit* maka jumlah permainan yang harus dilakukan pada uji craps ke-2 minimal harus lebih atau sama dengan 9415 kali.
4. Hasil pengujian terhadap sepuluh PRNG yang berasal dari tiga tipe PRNG yang berbeda menunjukkan uji craps baik uji 1 maupun uji-2 cukup efektif untuk mendeteksi bentuk distribusi dan independensi barisan yang dihasilkan suatu PRNG.

REFERENSI

[1] Kerckhoffs A., (1883), La Cryptographic Militaire. *Journal des Sciences Militaires* IX. 5-38.

[2] Marsaglia G., (1985), A current view of random number generator, *Keynote Addres, Proc.Statistics and Computer Science : 16th Symposium on the Interface, Atlanta*.

[3] Marsaglia G. & Tsang W.W., (2002), Some dificult-to-pass of randomness, *Journal of Statistical Software*. 7, Issue 3.

[4] Schneier B., (1996), Applied Cryptography : Protocols, Algorithms and Source Code in C 2nd Edition, John Wiley & Sons, Canada.

[5] Soejati Z., (1985), *Metode Statistika 2 Edisi 1*, Universitas Terbuka, Jakarta.