Verifikasi Pengacakan dan Pembagian Kartu pada Permainan Poker Online dengan menggunakan Secret Sharing Scheme

Jonathan Yudi Gunawan - 13518084
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
jonathanyudigun@gmail.com

***Abstrak*—Permainan poker *online* sering menimbulkan kecurigaan, apakah pembagian kartu dilakukan dengan adil atau tidak. Dengan menggunakan *secret sharing scheme*, verifikasi pembagian kartu dapat dilaksanakan. Karena setiap pemain tidak ingin membagikan isi kartu tangan mereka, maka kartu tangan setiap pemain dapat dianggap sebagai *share*. Kemudian di akhir permainan, *share* seluruh pemain dapat digabungkan untuk memverifikasi pembangkit bilangan acak semu yang digunakan untuk melakukan pembagian kartu.**

Kata kunci*—Poker *Online*, *Secret Sharing Scheme*, *Pseudo Random Number Generator*, *PRNG

I. Pendahuluan

Poker merupakan permainan kartu yang populer di banyak negara. Selain mengandalkan keterampilan, poker juga termasuk permainan yang mengandalkan keberuntungan. Hal ini disebabkan karena permainan poker bergantung pada pengacakan dan pembagian kartu yang dilakukan oleh *dealer*.

Seiring perkembangan teknologi yang semakin pesat, kini banyak permainan tradisional dapat dimainkan pada perangkat komputer, termasuk poker. Bahkan, poker pada komputer kini dapat dimainkan bersama-sama secara *online* melalui koneksi internet.

Tentu untuk menyelenggarakan permainan yang adil, diperlukan satu pihak yang berperan sebagai *dealer*. Pihak ini menggantikan peran *dealer* untuk melakukan pengacakan dan pembagian kartu, serta memandu berjalannya permainan. Namun, tidak jarang ditemukan penyelenggara poker *online* yang melakukan kecurangan dengan berbagai cara seperti mengacaukan pengacakan kartu.

Verifikasi perlu dilakukan untuk menjamin keabsahan permainan poker *online*. Verifikasi yang bagus sebaiknya dapat dilakukan dengan mudah oleh seluruh pemain tanpa mengacaukan alur permainan dan mengungkap pengacakan kartu sebelum selesainya permainan. Pada makalah ini akan dibahas pemanfaatan *secret sharing scheme* untuk melakukan verifikasi pengacakan dan pembagian kartu poker *online*.

II. Dasar Teori

A. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu "*cryptos*" yang artinya "yang tersembunyi" dan "*graphein*" yang artinya "tulisan". Menurut Menez, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. (Menez, 1996)

Di dalam kriptografi, terdapat empat tujuan yang ingin dicapai:

1. Terjaga kerahasiaannya (*confidentiality*),
2. Terjaga keasliannya (*data integrity*),
3. Yakin pengirim pesan asli (*authentication*), bukan pihak ketiga yang menyamar,
4. Pengirim pesan tidak dapat menyangkal (*non repudiation*) telah mengirim pesan

Di dalam kriptografi juga terdapat terminologi yang sering digunakan, yaitu:

1. Pesan
   Informasi yang dapat dibaca dan dimengerti maknanya (baik persepsi secara visual maupun audial). Nama lain: plainteks, *plain-image*, atau *plain-video*.
2. Pengirim
   Pengirim adalah subjek atau pihak yang mengirimkan sebuah pesan. Pengirim dapat berupa orang, komputer, mesin, dan lain-lain.
3. Penerima
   Penerima adalah subjek atau pihak yang menerima pesan dari pengirim. Penerima juga dapat berupa orang, komputer, mesin dan lain-lain.
4. Cipherteks
   Cipherteks adalah pesan yang telah disandikan sehingga lebih sulit untuk dibaca dan menjadi kurang bermakna lagi. Tujuannya adalah agar pesan tidak

dapat dibaca oleh pihak yang tidak berhak. Nama lainnya adalah kriptogram.

5. Enkripsi
   Enkripsi adalah proses untuk menyandikan sebuah plainteks menjadi cipherteks. Nama lainnya adalah *enciphering*.
6. Dekripsi
   Dekripsi adalah proses yang berlawanan dengan proses enkripsi. Proses dekripsi adalah proses untuk mengembalikan cipherteks menjadi plainteks semula. Nama lainnya adalah *deciphering*.
7. Cipher
   Cipher adalah algoritma yang digunakan untuk melakukan enkripsi atau dekripsi. Cipher merupakan sebuah fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan.
8. Kunci
   Kunci adalah parameter yang digunakan di dalam enkripsi dan dekripsi. Prinsip Kherkoff menyatakan semua algoritma kriptografi harus publik, sedangkan kunci harus rahasia.
9. Penyadap
   Penyadap adalah orang atau mesin yang mencoba menangkap pesan selama ditransmisikan. Nama lainnya adalah *enemy*, *adversary*, *intruder*, *interceptor*, ataupun *bad guy*.
10. Kriptanalisis
    Kriptanalisis adalah ilmu dan seni untuk memecahkan cipherteks menjadi sebuah plainteks tanpa mengetahui kunci yang digunakan. Orang yang melakukan kriptanalisis disebut sebagai kriptanalis.
11. Kriptologi
    Kriptologi adalah studi mengenai kriptografi dan kriptanalisis.

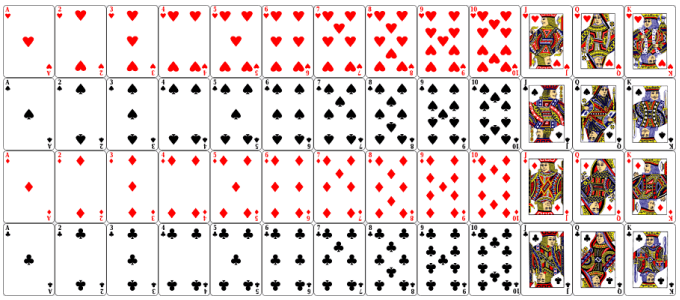
Kriptografi pada zaman dahulu hanya melakukan enkripsi pada huruf dan angka, dengan menggunakan kertas dan pena. Namun, pada zaman modern, kriptografi dapat dilakukan pada media selain huruf dan angka, bahkan pada media selain teks seperti gambar, video, audio, dll.

Untuk melakukan enkripsi pada media selain teks, biasanya dilakukan *encoding* pada file sehingga proses enkripsi dapat dilakukan dalam bentuk digital.

Contoh algoritma kriptografi kuno yang terkenal adalah *vigenere cipher*, *caesar cipher*, dll. Sedangkan contoh algoritma kriptografi modern yang terkenal adalah *RSA*, *Blowfish*, *DES*, dll.

B. Poker

Poker merupakan permainan kartu menggunakan dek standar, yakni berisi 52 kartu. Dek terdiri dari 13 tingkat atau pangkat dikombinasikan dengan 4 jenis suit. Contoh sebuah set dek standar dapat dilihat pada Gambar I.



Gambar I. Contoh Set Dek Standar 52 Kartu
(https://www.pngegg.com/en/png-nnrxg)

Terdapat beberapa istilah penting yang umum digunakan dalam permainan poker, antara lain:

1. *Dealer*
   Dealer atau bandar adalah seseorang yang bertugas membagikan kartu pada permainan poker. Bandar juga bertugas untuk menjaga jalannya permainan pada setiap rondenya.
2. *Community card* / *shared card*
   Community card atau kartu tengah adalah kartu yang dibuka di tengah meja. Setiap pemain dapat menggunakan kartu tengah sebagai bagian dari kombinasi kartu mereka. Kartu tengah berjumlah 5 kartu.
3. Fase *Pre-Flop*
   Fase *Pre-Flop* merupakan fase awal permainan, yakni fase pembagian dua kartu pada masing-masing pemain. Kartu ini disebut kartu tangan.
4. Fase *Flop*, *Turn*, dan *River*
   Fase *Flop* merupakan fase pembagian tiga kartu tengah pertama. Kemudian dilanjutkan dengan fase *Turn* untuk membuka kartu selanjutnya sehingga kartu tengah berjumlah empat kartu. Terakhir, dilanjutkan dengan fase *River* untuk membuka kartu tengah terakhir sehingga kartu tengah berjumlah lima kartu.
5. Fase *Showdown* / *Post-Flop*
   Fase *Showdown* / *Post-Flop* merupakan fase setelah fase *Flop*. Setiap pemain akan membuka kartu tangan mereka dan membandingkan total poin yang mereka peroleh. Pemenang akan ditentukan juga pada fase ini.

Permainan poker dimulai dengan fase *pre-flop*. Setelah itu, setiap pemain akan bermain secara bergiliran. Terdapat beberapa aksi yang dapat dilakukan oleh setiap pemain, yaitu:

1. *Open*
   Open dilakukan untuk membuka ronde taruhan yang mengharuskan setiap pemain selanjutnya pada ronde ini untuk melakukan taruhan atau menutup kartu mereka.
2. *Call*
   Call dilakukan untuk melakukan taruhan dengan nilai taruhan yang sama dengan nilai yang sebelumnya.

3. *Raise*
   Raise dilakukan untuk melakukan taruhan sekaligus meningkatkan nilai taruhan pada ronde saat ini.
4. *Check*
   Jika belum ada yang melakukan *open*, *check* dapat dilakukan untuk menghindari taruhan. Artinya, pemain ini belum menambahkan nilai taruhan dan ingin melihat terlebih dahulu bagaimana jalannya permainan.
5. *Fold*
   Fold dilakukan untuk menutup kartu dan mengundurkan diri dari permainan saat ini.

Setelah kelima kartu tengah dibuka, fase *post-flop* akan dijalankan. Kartu setiap pemain akan diurutkan berdasarkan kombinasi kartu mereka. Pemain dengan urutan tertinggi memenangkan permainan. Urutan kombinasi kartu dapat dilihat pada gambar II.

Gambar II. Urutan Kombinasi Kartu Poker
(https://thebestpokersitesonline.com/basics/poker-hands/)

C. Poker Online

Teknologi semakin maju. Melalui internet, orang-orang dapat bertemu dan berkumpul secara virtual. Hal ini memungkinkan permainan poker untuk dimainkan secara *online*.

Peran *dealer* yang sebelumnya dijalankan oleh manusia, kini dapat digantikan oleh komputer atau server. Pengacakan kartu juga dilakukan oleh server ini agar urutan kartu tidak dapat diketahui oleh pemain manapun. Kartu-kartu kemudian dibagikan secara virtual sebagai kartu digital pada layar komputer. Selanjutnya, alur permainan dipandu oleh komputer. Mulai dari pembagian kartu, pemilihan aksi setiap pemain, hingga penentuan pemenang permainan.

D. Pembangkit Bilangan Acak Semu / Pseudo Random Number Generator (PRNG)

Bilangan acak merupakan bilangan yang tidak dapat diprediksi nilainya. Bilangan acak sering digunakan di dalam kriptografi. Tidak ada prosedur komputasi yang dapat menghasilkan deret bilangan acak yang benar-benar sempurna / *truly random*. Bilangan acak yang dihasilkan dengan prosedur komputasi adalah bilangan acak semu / *pseudo-random*. Pembangkit bilangan acak semacam itu disebut juga sebagai pembangkit bilangan acak semu / *pseudo random number generator* (*PRNG*). *PRNG* bersifat deterministik, artinya bilangan acak dapat ditentukan asalkan nilai kuncinya / nilai umpannya / *seed*-nya diketahui.

Terdapat berbagai algoritma pembangkit bilangan acak semu seperti *Linear Congruential Generator* (*LCG*), *Blum Blum Shub* (*BBS*), pembangkit bilangan acak berbasis *logistic map*, dll. Pada makalah ini tidak akan diimplementasikan secara spesifik algoritma tertentu, namun perlu diingat bahwa nilai *seed* yang sama akan selalu menghasilkan sekuens bilangan acak yang sama.

E. Skema Pembagian Data Rahasia / Secret Sharing Scheme

Secret sharing scheme memungkinkan untuk memecah-mecah dan membagikan data rahasia ke beberapa pihak tanpa membocorkan data tersebut hingga pecahan data tersebut dikumpulkan menjadi satu.

Terdapat beberapa terminologi / istilah yang sering digunakan dalam *secret sharing scheme*, antara lain:

1. *Secret*
   Secret adalah data / informasi yang ingin dirahasiakan. Informasi dapat berupa *password*, kunci, PIN, pesan, file, dsb. Secret direpresentasikan sebagai sebuah bilangan bulat M.
2. *Share*
   Share merupakan hasil pembagian *secret*. *Secret* akan dipecah dan diolah menjadi beberapa share.
3. *Dealer*
   Dealer merupakan pihak yang melakukan pembagian *secret*.
4. Partisipan
   Partisipan adalah pihak yang memperoleh *share*.
5. Skema
   Skema ditentukan berdasarkan jumlah partisipan dan jumlah orang yang diperlukan untuk menggabungkan / merekonstruksi *share* menjadi *secret*. Contohnya skema(3, 8) artinya terdapat 8 partisipan dan hanya diperlukan 3 orang untuk melakukan rekonstruksi *share* menjadi *secret*.

Pertama-tama ditentukan skema yang akan digunakan. Kemudian, informasi rahasia akan terlebih dahulu diolah menjadi bilangan bulat M, selanjutnya disebut sebagai *secret*.

Selanjutnya, *share* dipecah sejumlah partisipan dengan menggunakan skema yang telah ditentukan.

Apabila ingin melakukan rekonstruksi *share* menjadi *secret*, sejumlah partisipan menggabungkan *share* mereka dan melakukan perhitungan untuk memperoleh *secret*.

Skema dapat diimplementasikan sebagai persoalan interpolasi. *Secret* dapat di-*encode* menjadi sebuah persamaan polinom dan share dapat direpresentasikan sebagai sebuah titik pada sistem koordinat yang dilalui oleh polinom tersebut. Masing-masing partisipan akan mendapat sebuah titik, namun tidak mengetahui persamaan polinom yang digunakan, hingga sejumlah partisipan memutuskan untuk menggabungkan titik-titik mereka.

III. Rancangan Solusi

Solusi yang diusulkan adalah pemain dapat melakukan verifikasi pengacakan dek kartu dengan menggunakan *secret sharing scheme* dengan Skema (N, N), dengan N adalah jumlah pemain yang berpartisipasi. *Share* dibagikan kepada pemain dalam bentuk kartu tangan pertama setiap pemain. Informasi yang dirahasiakan adalah *seed* dari algoritma *Pseudo Random Number Generator / PRNG* yang digunakan. Setelah permainan berakhir, seluruh pemain akan menggabungkan kartu pertama mereka untuk memperoleh *seed PRNG*. Kemudian, pemain dapat melakukan simulasi pengacakan dek kartu dengan menggunakan *seed* tersebut. Terakhir, verifikasi dapat dilakukan dengan mencocokkan N kartu pertama dengan kartu tangan kedua dari masing-masing pemain. Lima kartu selanjutnya juga harus sesuai dengan lima kartu tengah.

IV. Rancangan Implementasi

Pada bagian ini dibahas mengenai cakupan program dan rancangan detail implementasi pada setiap tahap atau fase permainan poker.

A. *Cakupan Implementasi*

Berikut cakupan implementasi program yang akan dibuat:

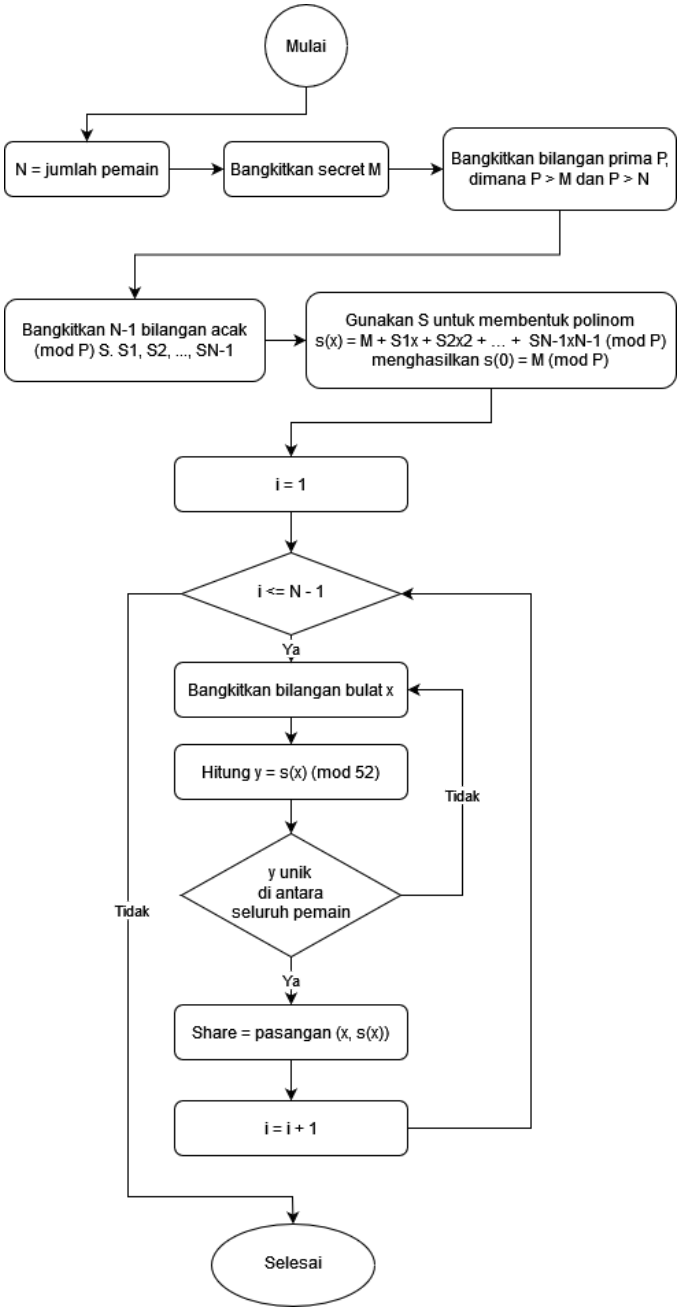
1. Mensimulasikan pengacakan dek kartu dengan seed tertentu.
2. Mensimulasikan pembagian *share* ke N pemain.
3. Mensimulasikan pembagian kartu ke N pemain, masing-masing 2 kartu.
4. Mensimulasikan pembagian 5 kartu tengah.
5. Menggabungkan N *share* untuk mengetahui informasi *seed*.
6. Melakukan verifikasi terhadap N kartu tangan kedua setiap pemain dan 5 kartu tengah.

Berikut hal-hal yang tidak diimplementasikan pada program:

1. Simulasi permainan poker
2. *Artificial Intelligence* untuk bot poker
3. *User Interface* grafis. Program akan dijalankan dengan antarmuka *command line* / *Command Line Interface*.

B. *Fase Pembangkitan Seed dan Share*

Pembangkitan *seed* dan *share* tiap pemain digambarkan melalui flowchart pada Gambar III.



Gambar III. *Flowchart* Pembangkitan *Seed* dan *Share*

C. *Fase Pengacakan Kartu / Pre-Flop*

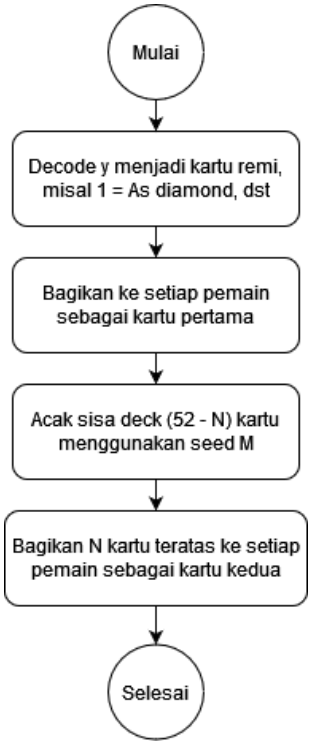
Pengacakan dan pembagian kartu digambarkan melalui *flowchart* pada Gambar IV.

D. *Fase Permainan / Flop, Turn, dan River dan Fase Penentuan Pemenang*

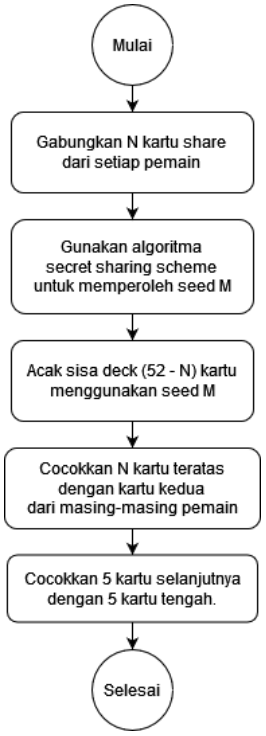
Fase permainan hanya melakukan pembukaan 5 kartu teratas sebagai kartu tengah. Ronde dalam permainan tidak akan disimulasikan. Program akan langsung menganggap permainan selesai setelah kartu tengah dibuka. Penentuan pemenang juga tidak disimulasikan pada program ini.

E. *Fase Verifikasi / Post-Flop*

Fase verifikasi digambarkan melalui *flowchart* pada Gambar V.



Gambar IV. *Flowchart* Pengacakan dan Pembagian Kartu (kiri)



Gambar V. *Flowchart* Verifikasi Pengacakan Kartu (Kanan)

V. Implementasi dan Uji Coba

Pada bagian ini dibahas mengenai implementasi dari rancangan yang telah dibahas pada bagian sebelumnya. Selain itu, dilakukan juga uji coba dengan menggunakan 3 alur berbeda, yakni alur normal, alur dealer melakukan pemilihan kartu yang dikeluarkan, dan alur dealer melakukan pengacakan dek dengan *seed* lain.

A. *Alur Normal 1*

Pengujian dilakukan dengan empat (4) orang pemain dengan variabel yang dibangkitkan secara acak. Hasil pembangkitan variabel dan hasil verifikasi dapat dilihat melalui Tabel I dan Tabel II.

TABEL I. Hasil Pembagian Kartu Alur Normal 1

N	4
M	57272
S1, S2, S3	76259, 78356, 65690
s(x)	57272.0 + 76259.0 x**1 + 78356.0 x**2 + 65690.0 x**3
x1, x2, x3, x4	31, 64, 54, 36
y1, y2, y3, y4	15, 36, 50, 48
z1, z2, z3, z4	19, 27, 35, 36
t1, t2, t3, t4, t5	38, 41, 16, 2, 45

TABEL II. Hasil Verifikasi Kartu Alur Normal 1

N	4
M'	57272
S1, S2, S3, S4	76259, 78356, 65690
s(x)	57272.0 + 76259.0 x**1 + 78356.0 x**2 + 65690.0 x**3
x1, x2, x3, x4	31, 64, 54, 36
y1, y2, y3, y4	15, 36, 50, 48
z'1, z'2, z'3, z'4	19, 27, 35, 36
t'1, t'2, t'3, t'4, t'5	38, 41, 16, 2, 45

Verifikasi berhasil dilakukan untuk permainan dengan empat (4) pemain dan alur pembagian kartu normal karena empat (4) kartu pertama (y1, y2, y3, y4) sesuai dengan empat (4) kartu pertama hasil acakan dengan menggunakan seed M' (y'1, y'2, y'3, y'4) serta 5 kartu selanjutnya (t'1, t'2, t'3, t'4, t'5) sesuai dengan 5 kartu tengah (t1, t2, t3, t4, t5).

B. *Alur Normal 2*

Pengujian dilakukan dengan enam (6) orang pemain dengan variabel yang dibangkitkan secara acak. Hasil pembangkitan variabel dan hasil verifikasi dapat dilihat melalui Tabel III dan Tabel IV.

TABEL III. Hasil Pembagian Kartu Alur Normal 2

N	6
M	6190
S1, S2, S3, S4, S5	80221, 82415, 18194, 92479, 49227
s(x)	6190.0 + 80221.0 x**1 + 82415.0 x**2 + 18194.0 x**3 + 92479.0 x**4 + 49227.0 x**5
x1, x2, x3, x4, x5, x6	2, 47, 92, 62, 59, 30
y1, y2, y3, y4, y5, y6	40, 30, 34, 48, 6, 48
z1, z2, z3, z4, z5, z6	30, 12, 50, 32, 39, 51
t1, t2, t3, t4, t5	44, 48, 20, 43, 45

TABEL IV. HASIL VERIFIKASI KARTU ALUR NORMAL 2

N	6
M'	6190
S1, S2, S3, S4, S5, S6	80221, 82415, 18194, 92479, 49227
s(x)	6190.0 + 80221.0 x**1 + 82415.0 x**2 + 18194.0 x**3 + 92479.0 x**4 + 49227.0 x**5
x1, x2, x3, x4, x5, x6	2, 47, 92, 62, 59, 30
y1, y2, y3, y4, y5, y6	40, 30, 34, 48, 6, 48
z'1, z'2, z'3, z'4, z'5, z'6	30, 12, 50, 32, 39, 51
t'1, t'2, t'3, t'4, t'5	44, 48, 20, 43, 45

Verifikasi berhasil dilakukan untuk permainan dengan 6 pemain dan alur pembagian kartu normal karena enam (6) kartu pertama (y1, y2, y3, y4, y5, y6) sesuai dengan 6 kartu pertama hasil acakan dengan menggunakan seed M' (y'1, y'2, y'3, y'4, y'5, y'6) serta 5 kartu selanjutnya (t'1, t'2, t'3, t'4, t'5) sesuai dengan 5 kartu tengah (t1, t2, t3, t4, t5).

C. Alur Dealer Nakal 1

Pengujian dilakukan dengan empat (4) orang pemain. Namun, setelah dek diacak, pembukaan kartu tengah tidak dilakukan sesuai urutan. Pada kasus ini pembukaan dilakukan dengan urutan kartu ke-2, 4, 6, 8, dan 10. Hasil pembangkitan variabel dan verifikasi dapat dilihat pada tabel V dan VI.

TABEL V. HASIL PEMBAGIAN KARTU ALUR DEALER NAKAL 1

N	4
M	44282
S1, S2, S3	97200, 7309, 9260
s(x)	44282.0 + 97200.0 x**1 + 7309.0 x**2 + 9260.0 x**3
x1, x2, x3, x4	56, 44, 20, 9
y1, y2, y3, y4	18, 2, 34, 47
z1, z2, z3, z4	17, 28, 47, 42
t1, t2, t3, t4, t5	37, 7, 14, 8, 36

TABEL VI. HASIL VERIFIKASI KARTU ALUR DEALER NAKAL 1

N	4
M'	44282
S1, S2, S3, S4	97200, 7309, 9260
s(x)	44282.0 + 97200.0 x**1 + 7309.0 x**2 + 9260.0 x**3
x1, x2, x3, x4	56, 44, 20, 9
y1, y2, y3, y4	18, 2, 34, 47
z'1, z'2, z'3, z'4	17, 28, 47, 42
(t'1, t'2, t'3, t'4, t'5)	7, 37, 8, 14, 39

Pada tabel V dan VI, meskipun N kartu kedua (z'1, z'2, z'3, z'4) sesuai dengan hasil acakan awal (z1, z2, z3, z4), namun lima (5) kartu teratas (t'1, t'2, t'3, t'4, t'5) tidak sesuai dengan lima (5) kartu tengah (t1, t2, t3, t4, t5). Maka, dapat disimpulkan bahwa terdapat kecurangan pada fase pembukaan kartu tengah, yakni fase permainan.

D. Alur Dealer Nakal 2

Pengujian dilakukan dengan empat (4) orang pemain. Namun, pengacakan dilakukan dengan seed selain M. Hasil pembangkitan variabel dan verifikasi dapat dilihat pada tabel VII dan VIII.

TABEL VII. HASIL PEMBAGIAN KARTU ALUR DEALER NAKAL 2

N	4
M	9634
S1, S2, S3	64134, 25337, 50000
s(x)	9633.0 + 64134.0 x**1 + 25337.0 x**2 + 50000.0 x**3
x1, x2, x3, x4	58, 1, 24, 87
y1, y2, y3, y4	33, 20, 13, 8
z1, z2, z3, z4	13, 21, 16, 7
t1, t2, t3, t4, t5	49, 46, 17, 12, 45

TABEL VIII. HASIL VERIFIKASI KARTU ALUR DEALER NAKAL 2

N	4
M'	9633
S1, S2, S3	64134, 25337, 50000
s(x)	9633.0 + 64134.0 x**1 + 25337.0 x**2 + 50000.0 x**3
x1, x2, x3, x4	58, 1, 24, 87
y1, y2, y3, y4	33, 20, 13, 8
(z'1, z'2, z'3, z'4)	31, 13, 28, 32
(t'1, t'2, t'3, t'4, t'5)	34, 24, 43, 19, 51

Pada tabel VI dan VII, terlihat bahwa terdapat perbedaan pada kartu tangan kedua dan kelima kartu tengah. Maka, dapat disimpulkan bahwa terdapat kecurangan pada fase awal permainan, yakni pada pembangkitan *seed* M yang digunakan untuk mengacak dek kartu.

VI. Kesimpulan dan Saran

Makalah ini membahas mengenai implementasi *secret sharing scheme* untuk melakukan verifikasi pengacakan dan pembagian kartu dek pada permainan poker *online*. Hasil yang didapat adalah skema ini dapat digunakan dan cocok untuk permainan poker karena pada dasarnya setiap orang akan memiliki kartu yang tidak akan dibagikan kepada pemain lain hingga berakhirnya permainan. Namun, masih diperlukan pengujian untuk mengetahui apakah ternyata ada celah yang dapat dimanfaatkan pemain untuk menebak pembagian kartu dari *share* yang dimilikinya.

Pranala Repository Github

Kode program dapat diakses melalui pranala berikut https://github.com/JonathanGun/online-poker-deck-shuffle-validation-using-secret-sharing-scheme

Ucapan Terima Kasih

Puji syukur penulis ucapkan kepada Tuhan yang Maha Esa karena berkat-Nya penulis dapat menyelesaikan makalah ini. Penulis juga mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen mata kuliah IF4020 Kriptografi tahun ajaran 2021/2022 yang telah memberikan ilmu dan pengalaman melalui mata kuliah ini. Selain itu, penulis juga mengucapkan terima kasih kepada keluarga serta teman-teman yang selalu memberi dukungan kepada saya dalam menjalankan perkuliahan.

Referensi

[1] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Pengantar Kriptografi. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2021-2022/Pengantar-Kriptografi-(2021).pdf. Diakses pada 11 Desember 2021.

[2] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Skema Pembagian data Rahasia (Secret Sharing Scheme). https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Skema-Pembagian-Data-Rahasia-(2018).pdf. Diakses pada 11 Desember 2021.

[3] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Pembangkit Bilangan Acak. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pembangkit-bilangan-acak-2020.pdf. Diakses pada 11 Desember 2021

[4] Kelasjudi. 2019. https://kelasjudi.wordpress.com/2019/09/06/istilah-dalam-permainan-poker-dan-urutan-kombinasi-kartunya-2/. Diakses pada 18 Desember 2021.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Desember 2021

Jonathan Yudi Gunawan

NIM 13518084