Implementasi Shamir Secret Sharing pada Aplikasi Silent Auction

Angelica Winasta Sinisuka - 13520097
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520097@std.stei.itb.ac.id

***Abstract*—Aplikasi *Silent Auction* membutuhkan kriteria, yaitu menjaga keamanan dari partisipan lelang. Agar menjaga identitas dari partisipan, maka diimplementasikan skema shamir secret key pada aplikasi ini serta hash-256 untuk menjaga keamanan dari tampering data shared key yang dihasilkan dari shamir secret sharing.**

Keywords—shamir secret sharing, hash-256, aplikasi silent auction

I. PENDAHULUAN

Silent auction merupakan auction yang dilakukan tanpa panduan dan dilakukan sebagai bentuk *fundrazining* untuk organisasi non profit. Auction ini mengumpulkan benda-benda yang disumbangkan seperti hadiah sertifikat, benda seni rupa, dan lainnya yang kemudian akan dibeli oleh partisipan auction ini. *Bidding* dilakukan melalui aplikasi sehingga setiap partisipan memasukkan nominal yang ingin diberikan untuk suatu barang yang diperagakan pada auction. Oleh karena itu, untuk memastikan privasi dari jumlah nominal yang dimasukkan oleh partisipan, maka diimplementasi shamir secret sharing pada aplikasi.

Secara tradisional, lelang dilakukan menggunakan basis secara kertas. Namun, masalah privasi tidak terjaga karena secara langsung informasi tersebut tampak dari pengelola kertas. Kemudian, perhitungan berbasis kertas dapat menyebabkan error dan masalah.

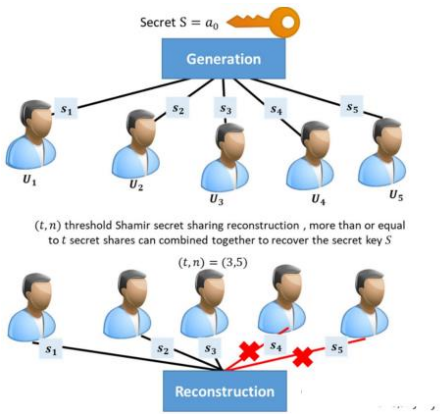
Shamir secret sharing merupakan teknik kriptografi yang membagi kunci menjadi beberapa bagian dan direkonstruksi kembali dengan minimal jumlah kunci yang sudah ditentukan. Keuntungan dengan menerapkan shamir secret sharing membantu dengan menghindari aksi yang tidak diotorisasi atau dimanipulasi karena memastikan tidak ada satu entitas dapat mengakses informasi secara keseluruhan. Kemudian data yang didistribusi disentralisasi dapat memitigasi keamanan dari mengeliminasi kebutuhan satu database yang disentralisasi. Terakhir, dapat memastikan bahwa tidak ada bias antara partisipannya karena informasi yang anonim.

Shamir secret sharing pada aplikasi dunia nyata diimplementasi pada *multi party computation*, *e-voting application*, dan *federated learning*. Selain dari itu, shamir secret sharing secara umum diimplementasi pada otentikasi terdistribusi, kontrol akses aman, dan manajemen kunci kriptografi.

II. TEORI DASAR

A. Shamir Secret Sharing

Variabel t merupakan ambang batas pembagian kunci untuk merekonstruksi kunci S dan variable t lebih kecil sama dengan n. Shamir secret sharing adalah metode pembagian secret S kepada n partisipan. Dari sembarang subset himpunan hasil pembagian secret S dengan jumlah t, maka dapat dikonstruksi S kembali. Namun, jika kurang dari t, kunci S tidak dapat direkonstruksi.



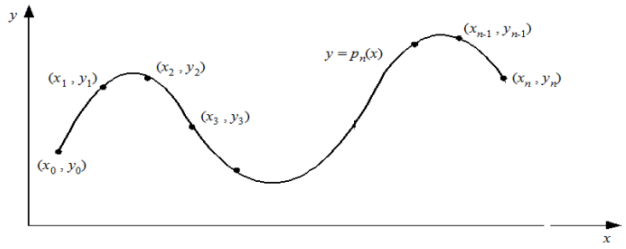
Gambar 1 Skema shamir secret sharing [1]

B. Skema Shamir Secret Sharing

Polinom interpolasi derajat n menggunakan persamaan sebagai berikut:

$$y = p_n(x) = a_0 + a_1x + a_2 x^2 + \ldots + a_nx^n \quad (1)$$

Persamaan (1) membutuhkan n+1 untuk menginterpolasikan titik-titik (x_0, y_0), (x_1, y_1), …, (x_n, y_n).



Gambar 2 Persamaan Interpolasi [1]

Algoritma

1. Bilangan prima p lebih besar dari kemungkinan nilai secret S dan jumlah n partisipan.
2. Pilih t-1 buah bilangan bulat secara acak dari bilangan-bilangan yang lebih kecil dari p (bilangan prima). Bilangan-bilangan ini akan kita sebut sebagai a1, a2, ..., at-1
3. Buatlah polynomial dengan nama f(x). Polinomial ini terdiri dari S, sebuah konstanta yang nilainya bebas. X, bariabel yang nilanya berubah-ubah. Bilangan-bilangan a1, a2, …, at-1 dikalikan dengan pangkat x yang sesuai. Kemudian t-1 sebagai pangkat tertinggi dari variable x.
4. Operasi polinomial dilakukan modulo p. Pastikan bahwa nilai polinomial f(x) sama dengan S ketika x sama dengan 0. Ini dituliskan sebagai **f(0) ≡ S (mod p)**.
5. Dengan n partisipan, dipilin nilai bilangan bulat berbeda untuk x1, x2, …, xn (mod p) dan setiap orang mendapatakn share (xi, yi) dari **yi ≡ f(xi) (mod p)**

C. Hash

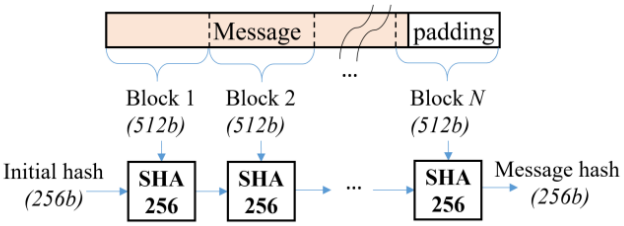
Hash merupakan algoritma matematika yang menerima input data dengan Panjang yang random sebagai input dan dipetakan ke panjang tertentu dalam bentuk teks sebagai output [2]. Fungsi hash kriptografi diklasifikasikan menjadi dua kelas, yaitu Manipulation Detection Code (MDC) yang menerima satu parameter, yaitu pesan input dan Message Authentication Code (MAC) yang menggunakan menggunakan 2 input berbeda, yaitu pesan input dan kunci [2].

Syarat yang dimiliki dari hash untuk keamanan adalah sebagai berikut:

- One-way function yaitu membutuhkan fungsi hash H yang menghasilkan h, sulit atau membutuhkan komputasi yang besar untuk mencari input m untuk menemukan h dari fungsi H. Sehingga hashing dapat dilakukan ke satu arah, untuk mendapatkan nilai hash, tetapi tidak sebaliknya.
- Target collision resistance, yaitu karaktersitik dari fungsi hash H dari input m tidak mendapatkan input lain m' hingga H(m) = H(m')
- Collision resistance, yaitu karaktersitik yang dibutuhkan dari fungsi hash H untuk mendapatkan dua input m dan m' yang mana m tidak sama dengan m', tetapi H(m) = H(m')
- Deterministic, yaitu karakteristik dari fungsi hash H selalu menghasilkan output h yang sama dari input m.
- Avalanche effect, yaitu karakterstik dari fungsi hash H, jika merubah satu bit dari input, akan menghasilkan perubahan yang besar pada output.
- Hash speed, adalah karakterstik fungsi hash yang idealnya mempunyai kemampuan untuk beroperasi dalam kecepatan yang tinggi.

D. Hashing Pesan Menggunakan SHA-256

SHA-256 merupakan fungsi hash yang mempunyai output dengan panjang 256 bit. Fungsi ini termasuk fungsi hash tanpa kunci, yaitu jenis Manipulation Detection Code (MDC) [3]. Algoritma dari SHA-256 adalah sebagai berikut



Gambar 3 Proses hasil SHA-256 pada pesan [4]

Algoritma ini bekerja secara berulang, memproses pesan input blok demi blok. Berikut adalah langkah-langkah dasar dari algoritma SHA-256 secara berturut-turut:

1. Pra-pemrosesan

- Padding: Pesan input di-pad dengan bit 1, diikuti oleh bit 0 sebanyak yang diperlukan untuk membuat panjang pesan menjadi kelipatan 512 bit.
- Penambahan panjang pesan: Panjang pesan asli ditambahkan ke akhir pesan yang dipad.

2. Fungsi Kompresi

Pesan yang dipad dibagi menjadi blok 512-bit. Setiap blok diproses dengan menggunakan fungsi kompresi yang terdiri dari 8 putaran. Setiap putaran terdiri dari 4 operasi dasar:

- Fungsi Pilihan: Fungsi ini memilih salah satu dari 4 fungsi hash non-linear berdasarkan putaran saat ini.

- Fungsi Majority: Fungsi ini mengambil mayoritas dari 3 input.
- Fungsi Tambah (Add): Fungsi ini menambahkan dua input.
- Fungsi Rotasi Kiri: Fungsi ini memutar bit input ke kiri dengan jumlah bit yang ditentukan.

3. Nilai Hash Akhir

Nilai hash akhir adalah nilai hash dari blok terakhir pesan input. Nilai ini direpresentasikan sebagai string 256 karakter hex.

E. Silent Auction

Silent Auction merupakan suatu acara yang mana benda atau jasa ditampilkan agar partisipan dapat melakukan lelang pada benda tersebut. Hal ini diam karena tidak ada yang memimpin selama pelelangan. Setiap barang biasanya terdapat kertas atau dapat melakukan bidding melalui website atau aplikasi. Ketika waktu sudah selesai, maka setiap aplikasi biasanya terkunci yang kemudian akan diumumkan pemenangnya.

Silent auction dilakukan karena lingkungan yang ingin diciptakan lebih santai sehingga partisipan dapat fokus ke benda-benda yang dianggap menarik perhatian dan dilakukan secara sungguh-sungguh tanpa interferensi dari pihak lain. Kemudian penyelenggaraan lelang tidak membutuhkan sumber daya yang lebih seperti mik, atau pembawa acara lelang.

F. Kriptografi

Kriptografi adalah ilmu dan praktik tentang menjaga kerahasiaan informasi dengan menggunakan teknik pengkodean. Tujuan utama kriptografi adalah untuk melindungi informasi dari pihak yang tidak berwenang, baik saat informasi disimpan, dikirim, atau diproses.

Kriptografi bekerja berdasarkan beberapa prinsip dasar, yaitu:

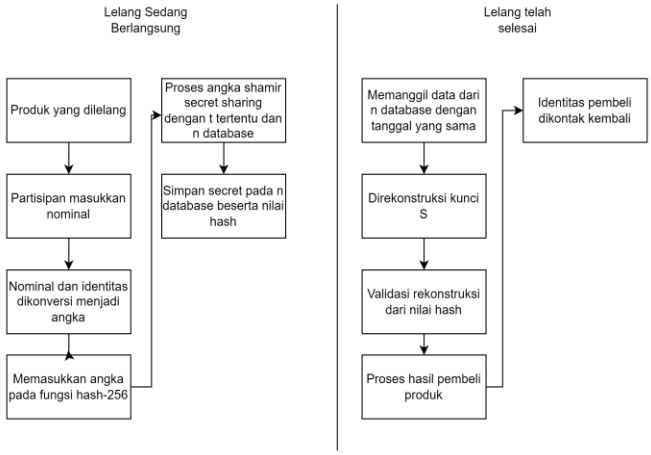
- Kerahasiaan: Informasi hanya dapat dibaca oleh pihak yang berwenang.
- Keutuhan: Informasi tidak dapat diubah oleh pihak yang tidak berwenang.
- Otentikasi: Pengirim informasi dapat diverifikasi.
- Non-repudiasi: Pengirim informasi tidak dapat menyangkal bahwa mereka telah mengirim informasi.

III. RANCANGAN SOLUSI

A. Deskripsi

Silent auction memiliki fitur untuk registrasi dan login. Kemudian partisipan yang telah login dapat melihat benda-benda yang ditunjukkan pada lelang. Jika partisipan ingin membeli, maka akan dimasukkan nominal tertentu. Lalu partisipan akan mengirim nominal untuk benda tersebut. Kemudian secret dari shamir secret sharing akan dibangkitkan berdasarkan nominal dan identitas dari pengirim. Kemudian akan digunakan beberapa database untuk menyimpan secret sharing key. Jika lelang sudah selesai, perhitungan akan dilakukan dari rekonstruksi secret dari data beberapa database. Setelah direkonstruksi, akan dibandingkan hasil hashing dari 256 untuk memvalidasi adanya tampering. Hasil akan ditunjukkan jika sudah selesai pada akhir acara beserta pemenangnya.

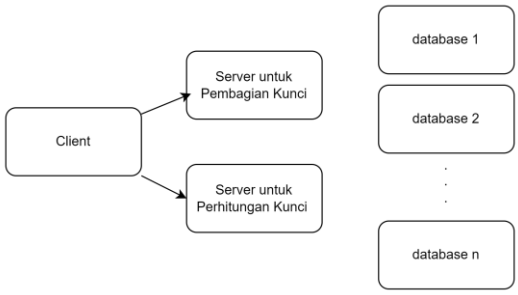
B. Skema Shamir Secret Sharing pada Aplikasi



Gambar 4 Skema Validasi dan Shamir Secret Sharing pada Aplikasi

Desain untuk meyimpan privasi atau jumlah nominal yang dikirim partisipan dari gambar 4. Fungsi hash yang digunakan untuk validasi adalah hash-256. Kemudian skema shamir secret sharing pada nominal dan identitas.

Partisipan merupakan pembeli dari lelang. Kemudian pada skema “lelang yang telah selesai”, partisipan pada tahap ini adalah penyelenggara acara. Validasi dilakukan pada server. Skema komunikasi antara client dengan server adalah sebagai berikut:



Gambar 4 Skema komunikasi client dan server

Proses yang dilakukan pada masing-masing bagian adalah sebagai berikut:

1. Pada client, partisipan lelang akan memasukkan nominal dan submit.
2. Client mengirimkan nilai nominal, identitas, dan produk.
3. Server menerima request dari client. Diasumsikan input dari user benar dan tidak diubah.
4. Server melakukan proses hashing, dan pengiriman tiap secret ke database yang berbeda-beda.
5. Setelah lelang selesai, server memanggil setiap data dari tiap database.
6. Setelah rekonstruksi kunci S, maka S dijadikan sebagai input untuk fungsi hash H.
7. Hasil output dari fungsi hash H divalidasi dari hashing sebelumnya.
8. Dilakukan ranking untuk produk tertentu.
9. Pemenang untuk setiap produk dikirim balik

Jika terjadi kesalahan dalam verifikasi. Maka akan dilakukan request ulang pada fungsi. Dalam interasi tertentu, dan dalam iterasi tertentu tidak berhasil, maka response yang dikembalikan adalah gagal.

C. Implementasi

Implementasi dilakukan dengan menggunakan Bahasa python dengan membuat 6 buah kelas, yaitu client, server, produk, objek database, database, dan databases. Berikut merupakan atribut dan metode yang dimiliki, yaitu:

1. Kelas client, kelas ini memiliki atribut nomor_id, nomor telepon, dan nama.
2. Kelas server, kelas ini mempunyai metode eksekusi shamir secret sharing, hashing, dan penyimpanan data dalam database.
3. Kelas objek_database, kelas ini memiliki atribut tanggal, kunci secret, dan nilai hash.
4. Kelas database, kelas ini merupakan database yang menyimpan objek database.
5. Kelas product, kelas ini memiliki atribut nama dan id
6. Kelas databases,kelas ini memiliki atribut semua daftar database.

IV. PENGUJIAN DAN ANALISIS

Pengujian dilakukan dengan menjalankan beberapa skenario sebagai berikut, yaitu:

1. Submit order dengan nilai bid yang bervariasi untuk beberapa item. Kemudian mengembalikan pemenang dari bidding tersebut.
2. Melakukan perubahan pada nilai secret key pada salah satu database, tetapi masih melebihi sama dengan nilai threshold untuk merekonstruksi secret key.
3. Melakukan perubahan pada salah satu kunci yang jumlah perubahan kurang dari ambang batas untuk merekonstruksi kunci kembali.
4. Melakukan perubahan pada semua hash key pada hash key yang sama.
5. Melakukan perubahan pada semua nilai secret key dengan nilai yang sama.
6. Melakukan perubahan pada hash key yang sama diatas threshold.
7. Melakukan perubahan pada hash key yang sama dibawah threshold.

A. Hasil Pengujian

Pada program, dideklarasi terlebih dahulu jumlah produk, user, database, nilai t (ambang batas rekonstruksi kunci), nilai n yang diasumsikan sebagai jumlah database yang dimiliki, sebagai berikut:

```
num_database = 5
threshold = 3
num_users = 5
num_products = 5
```

Pada kasus uji pertama, masing-masing user akan memberikan bidding pada setiap produk dengan nilai urutan produk dan urutan user yang sama merupakan bidder tertinggi.

```
BID WINNERS
================================
Product:  Product0 ( 133021 )
Identity:  User0 ( 862421 )
Nominal:  1000000000

Product:  Product1 ( 365871 )
Identity:  User1 ( 686000 )
Nominal:  1000000000

Product:  Product2 ( 814099 )
Identity:  User2 ( 582320 )
Nominal:  1000000000

Product:  Product3 ( 286111 )
Identity:  User3 ( 705454 )
Nominal:  1000000000

Product:  Product4 ( 698257 )
Identity:  User4 ( 462224 )
Nominal:  1000000000
```

Gambar 5 Output Program Hasil Lelang Kasus Satu

Dari hasil output diatas, shared key yang dipecahkan menjadi lima yang kemudian direkonstruksi kembali menjadi identitas, produk, dan nominal dapat dilakukan.

```
Hash result is not the same on database Database0. Data might be corrupted.
```

Gambar 6 Output Program Hasil Lelang Kasus Dua

Dari hasil output diatas, tampak ketika mengubah satu kunci, jika ada kunci yang diubah nilai hash tidak akan sama, dan konstruksi tidak tercapai. Namun, akan diiterasi dengan mencobakan semua kombinasi hingga nilai hash adalah sama untuk memastikan konstruksi S dapat dibuat walaupun diadakan korupsi kunci satu pada database satu. Hal ini akan mengeluarkan output yang sama seperti pada gambar 5. Apabila tidak ada nilai hash untuk dibandingkan, konstruksi tetap dapat dilakukan, tetapi nilai hasil konstruksi berbeda dengan originalnya yang memungkinkan menunjuk identitas pemenang bidder yang berbeda. Agar hal ini tidak terjadi maka diimplementasikan hashing agar korupsi pada key tidak dimasukkan ke dalam fungsi rekonstruksi.

```
not enough points for a unique interpolation
```

Gambar 7 Output Program Hasil Lelang Kasus Dua

Dari hasil output diatas, ketika mengubah 3 shared key dengan nilai yang sama, atau nilai yang asal, didapatkan hasil seperti yang diatas. Oleh karena itu, hasil yang akan dikembalikan dari hasil bidding untuk produk itu tidak ada. Apabila dikembalikan yang tidak rusak datanya, maka kemungkinan bidder tersebut bukan yang tertinggi.

```
Not enough secrets to recover the order
```

Gambar 8 Output Program Hasil Lelang Kasus 4

Berdasarkan nilai diatas, rekonstruksi tidak dapat dilakukan jika mengubah seluruh nilai hash pada data tertentu.

```
Hash result is not the same on database Database0. Data might be corrupted.
```

Gambar 9 Output Program Hasil Lelang Kasus 5

Berdasarkan nilai diatas, jika secret key, diubah dengan nilai yang sama, maka hasil yang didapatkan adalah gambar 8. Namun, jika diubah dengan nilai secret key dari objek yang berbeda. Hasil yang akan didapatkan adalah gambar 9. Hal ini mengartikan bahwa rekonstruksi berhasil dengan menggunakan secret key yang lain, tetapi karena hashing. Maka data terkorupsi tidak dikembalikan kepada pengguna.

```
BID WINNERS
========================================
Product:  Product0 ( 491929 )
Identity:  User0 ( 479708 )
Nominal:  1000000000

Product:  Product1 ( 965011 )
Identity:  User1 ( 143874 )
Nominal:  1000000000

Product:  Product2 ( 815099 )
Identity:  User2 ( 160255 )
Nominal:  1000000000

Product:  Product3 ( 209938 )
Identity:  User3 ( 578522 )
Nominal:  1000000000

Product:  Product4 ( 209216 )
Identity:  User4 ( 886352 )
Nominal:  1000000000
```

Gambar 10 Output Program Hasil Lelang Kasus 6

Berdasarkan output diatas, didapatkan bahwa rekonstruksi berhasil dilakukan. Hal ini terjadi karena terdapat 2 kunci yang tidak valid. Hanya 3 lainnya valid dan dapat direkonstruksi kembali. Oleh karena itu, output yang dihasilkan adalah benar.

```
Not enough secrets to recover the order
```

Gambar 11 Output Program Hasil Lelang Kasus 7

Berdasarkan output diatas, keluaran yang dihasilkan tidak dapat dilakukan karena tidak dapat direkonstruksi kembali kunci karena adanya nilai hash yang berbeda. Jumlah threshold kunci yang valid dibawah 3 sehingga keluaran yang dihasilkan adalah seperti gambar 11.

V. KESIMPULAN DAN SARAN

Dari hasil diatas, implementasi dari shamir secret sharing dapat diwujudkan pada aplikasi shamir secret sharing dengan menggunakan hashing untuk memastikan tidak ada *tamper* pada secret key di shamir secret sharing. Hal ini dilakukan dengan membagi hasil submit partisipan menjadi n kunci yang kemudian disimpan *message digest.* Ketika merekonstruksi, data akan dipanggil dari setiap database sehingga penyimpanan data tidak tersentralisasi, tetapi terdistribusi untuk menjaga keamanan jika salah satu database terbocorkan datanya, informasi yang diperoleh tidak ada maknanya. Hashing digunakan untuk menjaga integritas dari shared key. Sehingga ketika direkonstruksi kembali oleh shamir secret key, dapat divalidasi kembali menggunakan fungsi hash. Oleh karena itu kriteria yang berhasil dijaga dalam hal ini adalah integritas.

Hal yang belum dapat ditangani dalam implementasi adalah pengiriman request ke server yang aman. Hal ini dapat dilakukan dengan membuat shared key antara server dengan client yang kemudian dienkripsi selama melakukan request dan didekripsi oleh server melalui shared key. Kemudian pada pemrosesan yang dilakukan pada server, identitas yang melalukan lelang bisa terjaga dengan mengoperasikan perhitungan menggunakan teknik enkripsi homomorfik. Anjuran implementasi ini masih belum dilakukan pada aplikasi sebenarnya. Oleh karena itu, sangat dianjurkan untuk mengimplementasi secara langsung pada website atau aplikasi.

LINK SOURCE CODE

https://github.com/yoshibeside/tugas_akhir_makalah_kriptografi.git

UCAPAN TERIMA KASIH

Penulis mengucap Syukur kepada Tuhan yang Maha Esa karena ata rahmatnya penulis dapat menyelesaikan makalah ini. Penulis mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T sebagai dosen pengajar Mata Kuliah IF4020 Kriptografi yang telah mengajarkan berbagai teknik kriptografi dan pengetahuan umum sehingga penulis dapat menyelesaikan makalah ini dengan baik.

DAFTAR PUSTAKA

[1] Munir. Rinaldi 2024. Skema Pembagian Data Rahasia. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/35-Skema-Pembagian-Data-Rahasia-2024.pdf

[2] Macharia, Wahome. (2021). Cryptographic Hash Functions. https://www.researchgate.net/publication/351837904_Cryptographic_Hash_Functions

[3] The Cryptographic Hash Function. (n.d). SHA-256.pdf (stormhub.org)

[4] Tran, Thi Hong & Hoai Luan, Pham & Nakashima, Yasuhiko. (2021). A High-Performance Multimem SHA-256 Accelerator for Society 5.0. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3063485.

[5] What is a Silent Auction, and How Does It Work?. (2023). https://www.silentauctionpro.com/blogs/what-is-a-silent-auction.php

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, 12 Juni 2024

Angelica Winasta Sinisuka (13520097)