Implementasi Tanda Tangan Digital pada Tiket Konser Coldplay

Mahesa Lizardy - 13520116
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13520116@std.stei.itb.ac.id

***Abstract*—Penyelenggaraan konser world tour Coldplay "Coldplay MUSIC of the SPHERES" di Jakarta menarik perhatian masyarakat Indonesia. Namun, dalam kehebohan tersebut juga muncul kasus penipuan terkait penjualan tiket. Untuk mengatasi masalah ini dan menjaga integritas serta kepercayaan penggemar, penggunaan tanda tangan digital menjadi solusi yang efektif. Tanda tangan digital digunakan untuk melindungi tiket konser dari pemalsuan, duplikasi, atau manipulasi yang merugikan penyelenggara acara, artis, dan penonton. Dengan menerapkan teknologi kriptografi seperti algoritma hash SHA-256 dan kriptografi kunci publik seperti ElGamal, keamanan dan integritas tiket dapat terjaga dengan baik. Penerapan tanda tangan digital pada tiket konser Coldplay memberikan pengalaman yang lebih aman dan nyaman bagi pengguna serta melindungi penyelenggara acara dari penipuan dan penggunaan tiket ilegal.**

Keywords—ElGamal, ticket, digital signature

I. Pendahuluan

Baru-baru ini masyarakat Indonesia dihebohkan dengan kedatangan Coldplay ke Jakarta untuk melakukan world tour Coldplay MUSIC of the SPHERES. Acara ini telah menjadi sorotan utama bagi penggemar musik di seluruh negeri, yang tidak sabar untuk menyaksikan penampilan energik dan spektakuler dari band terkenal ini.

Namun, di tengah kehebohan ini, juga muncul berbagai kasus penipuan terkait penjualan tiket. Seiring dengan popularitas acara tersebut, penipu-penipu tak bertanggung jawab mencoba memanfaatkan antusiasme penggemar dengan menawarkan tiket palsu, tiket dengan harga yang jauh di atas nilai sebenarnya, atau bahkan melakukan aksi penipuan online.

Keberadaan penipuan semacam itu telah memicu kekhawatiran dan kebingungan di kalangan penggemar yang berharap untuk mendapatkan tiket dengan aman dan sah. Namun, untuk menjaga integritas dan kepercayaan penggemar, langkah-langkah keamanan perlu diambil. salah satu langkah keamanan yang dapat diambil yaitu dengan menerapkan tanda tangan digital

Tanda tangan digital adalah metode untuk memverifikasi keaslian dan integritas suatu dokumen elektronik atau data. Dalam konteks tiket konser Coldplay, tanda tangan digital digunakan untuk melindungi tiket dari pemalsuan, duplikasi, atau manipulasi yang dapat merugikan penyelenggara acara, artis, dan penonton.

Dalam praktiknya, implementasi tanda tangan digital pada tiket konser Coldplay dapat melibatkan penggunaan teknologi kriptografi, seperti algoritma kunci publik (seperti ElGamal) atau algoritma kunci simetris (seperti AES) untuk menghasilkan tanda tangan digital yang aman dan tidak dapat dipalsukan

Salah satu manfaat utama dari implementasi tanda tangan digital pada tiket konser Coldplay adalah peningkatan keamanan. Dengan menggunakan teknologi enkripsi yang kuat, tanda tangan digital dapat melindungi tiket dari pemalsuan atau duplikasi yang sering terjadi dalam industri hiburan. Setiap tiket akan memiliki tanda tangan digital yang unik dan sulit untuk dipalsukan, sehingga mempersulit upaya penipuan.

Tanda tangan digital juga memastikan integritas tiket. Data tiket, termasuk informasi acara, tanggal, waktu, dan tempat, dapat dienkripsi dan ditambahkan ke dalam tanda tangan digital. Dengan demikian, setiap perubahan atau manipulasi pada tiket akan terdeteksi, sehingga menjaga integritas informasi yang terkandung dalam tiket.

Dengan adopsi tanda tangan digital pada tiket konser Coldplay, pengguna dapat merasakan pengalaman yang lebih aman, terpercaya, dan nyaman dalam membeli dan menggunakan tiket. Penyelenggara acara dan artis juga akan mendapatkan manfaat dalam hal perlindungan terhadap penipuan dan penggunaan tiket yang tidak sah.

II. Dasar Teori

A. Tanda Tangan Digital

Sejak zaman dahulu, tanda tangan sudah dipergunakan untuk otentikasi terutama dokumen cetak. tanda tangan mempunyai karakteristik sebagai berikut. Pertama, tanda tangan merupakan bukti otentik yang menunjukkan identitas individu atau entitas yang melakukan tanda tangan. Ini memastikan bahwa dokumen tersebut berasal dari sumber yang sah dan dapat dipercaya. Tanda tangan juga memiliki

sifat yang tidak dapat dipindahkan untuk digunakan ulang, sehingga mencegah pemalsuan atau penggunaan yang tidak sah. Dokumen yang telah ditandatangani tidak dapat diubah tanpa meninggalkan jejak atau melanggar integritasnya. Terakhir, tanda tangan juga memiliki kekuatan hukum yang kuat, karena sulit untuk menyangkal keaslian tanda tangan tersebut.

Tanda-tangan untuk data digital dinamakan tanda-tangan digital (*digital signature*). Dalam konteks kriptografi tanda tangan digital tidak sama dengan tanda tangan yang di-digitalisasi (*digitized signature*) dengan cara dipindai atau difoto. Melainkan tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci yang diberikan. Perbedaanya adalah tanda tangan seseorang pada dokumen cetak akan selalu sama apapun isi dokumen nya, sedangkan tanda tangan digital akan berbeda-beda antara satu pesan dengan pesan lainnya atau antara satu kunci dengan kunci yang lain.

Dalam tanda tangan digital terdapat 2 proses utama yaitu menandatangani pesan (*signing*) dan memverifikasi pesan (*verification*). proses menandatangani pesan adalah proses dilakukan pemberian tanda tangan digital pada pesan. Sedangkan pada proses *verification* adalah memeriksa keabsahan tanda tangan digital yang terdapat pada pesan. Terdapat dua cara yang dapat dilakukan untuk menandatangani pesan yaitu mengenkripsi pesan untuk pesan rahasia dan menggunakan kombinasi fungsi hash (hash function) dan kriptografi kunci-publik untuk pesan yang tidak perlu rahasia

Dalam konteks tanda tangan digital, terdapat beberapa metode atau algoritma kriptografi yang umum digunakan, antara lain RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), dan ElGamal. RSA, yang menggunakan konsep faktorisasi bilangan bulat, telah menjadi salah satu algoritma tanda tangan digital yang paling populer dan luas digunakan. Algoritma DSA, yang dikembangkan oleh National Institute of Standards and Technology (NIST), juga dikenal karena kecepatan dan efisiensinya dalam menghasilkan dan memverifikasi tanda tangan digital. Sementara itu, ElGamal, yang didasarkan pada kesulitan masalah diskrit logaritma, menawarkan keamanan yang kuat dan telah digunakan dalam berbagai protokol keamanan. Ketiga metode ini memiliki keunggulan dan kelemahan masing-masing, dan pilihan algoritma yang tepat tergantung pada kebutuhan keamanan, kinerja, dan implementasi yang diinginkan dalam konteks penggunaan tanda tangan digital.

B. ElGamal

Algoritma Elgamal dibuat oleh Taher Elgamal (1985). Pertama kali dikemukakan di dalam makalah berjudul "A public key cryptosystem and a signature scheme based on discrete logarithms". Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Persoalan logaritma diskrit tersebut adalah sebagai berikut, jika p adalah bilangan prima dan g dan y adalah sembarang bilangan bulat, carilah x sedemikian sehingga

$$g^x \equiv y \ (mod\ p)$$

Dalam algoritma ElGamal terdapat beberapa properti sebagai berikut:

1. Bilangan prima (p)
2. bilangan acak, g (g < p, g adalah akar primitif dari p)
3. bilangan acak x ($2 \leq x \leq p - 2$) (kunci privat)
4. $y = g^x \bmod p$ (kunci publik)
5. m (plainteks)
6. a dan b (cipherteks)

Properti tersebut ada yang bersifat rahasia dan ada yang tidak. nilai bilangan prima, bilangan acak, kunci publik dan cipherteks bersifat tidak rahasia. Sedangkan nilai kunci privat bersifat rahasia. Sedangkan m bisa bersifat rahasia atau tidak rahasia bergantung pada penggunaanya

Pada Algoritma ElGamal terbagi menjadi tiga prosedur yaitu prosedur pembangkitan kunci, prosedur *signing*, dan prosedur *verification*. Pada prosedur pembangkitan kunci adalah tahapan yang dilakukan adalah sebagai berikut.

1. Pertama-tama akan dipilih panjang kunci N.
2. Pilih N-bit bilangan prima p.
3. Pilih generator g < p dari grup multiplikatif dari bilangan bulat modulo p
4. Pilih bilangan acak x diantara $2 \leq x \leq p - 2$ yang akan menjadi kunci privat.
5. Hitung nilai $y = g^x \bmod p$ untuk mendapatkan kunci publik.

Pada prosedur ini akan dihasilkan kunci publik berupa (p, g, y) dan kunci privat x. Selanjutnya, pada prosedur menandatangani pesan untuk pesan (m) tahapan yang dilakukan adalah sebagai berikut.

1. Pilih nilai random k dimana $0 < k < p - 1$ dan gcd(k, p-1)
2. Hitung nilai $r \equiv g^k \pmod p$
3. Hitung nilai $s \equiv (H(m) - xr)k^{-1} \pmod{p-1}$ dengan H(m) merupakan pesan m yang sudah dihash

Pada proses ini akan dihasilkan pasangan (r,s) merupakan digital signature dari m. Selanjutnya, pada prosedur memverifikasi tanda tangan digital tahapanya adalah sebagai berikut.

1. Cek nilai $0 < r < p$ dan $0 < s < p - 1$, jika nilai r dan s tidak terletak pada interval tersebut maka tanda tangan digital tidak sah / ditolak
2. Hitung $v1 = y^x r^s \bmod p$
3. Hitung $v2 = g^{H(m)} \bmod p$
4. Cek v1 = v2

Jika nilai v1 dan v2 sama maka verifikasi berhasil atau tanda tangan dapat dipastikan valid. Jika tidak sama maka verifikasi gagal atau tanda tangan tidak valid

C. SHA256

SHA-256 (Secure Hash Algorithm 256-bit) adalah sebuah fungsi hash kriptografis yang termasuk dalam keluarga algoritma Secure Hash Algorithm (SHA-2). Fungsi hash ini

digunakan untuk menghasilkan nilai hash dengan panjang 256-bit dari input data yang diberikan.

SHA-256 menggunakan serangkaian operasi matematika dan logika yang kompleks untuk menghasilkan nilai hash yang unik dan tidak dapat diprediksi. Proses penghitungan SHA-256 melibatkan pemecahan input data menjadi blok-blok yang lebih kecil, dan setiap blok diolah secara iteratif menggunakan transformasi yang melibatkan operasi bitwise, permutasi bit, dan fungsi logika seperti XOR dan AND.

Keamanan SHA-256 didasarkan pada sifat-sifat kriptografis seperti ketahanan terhadap *collision*, di mana sangat sulit untuk menemukan dua input yang menghasilkan nilai hash yang sama. Selain itu, SHA-256 juga memiliki sifat ketahanan terhadap perubahan kecil pada input data, sehingga perubahan kecil pada data input akan menghasilkan nilai hash yang berbeda secara signifikan.

III. Rancangan Solusi dan Implementasi

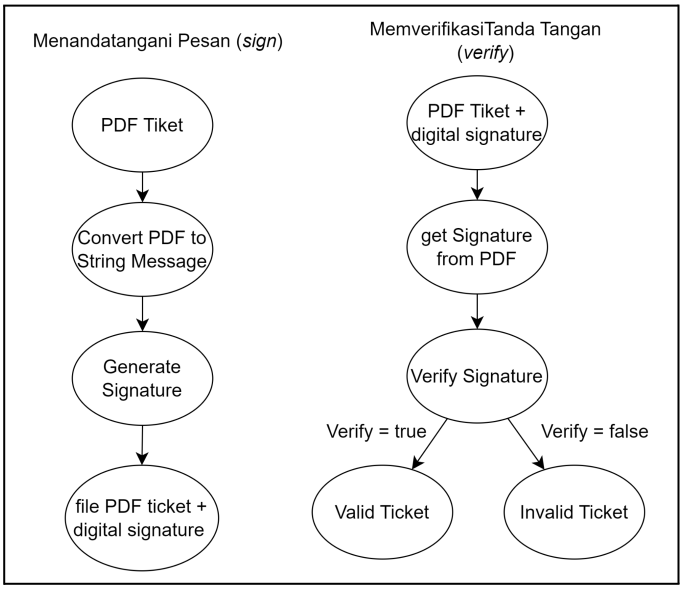
A. Deskripsi Umum Solusi

Permasalahan ini akan diselesaikan dengan menggunakan tanda tangan digital dengan metode kombinasi fungsi hash (hash function) dan kriptografi kunci-publik. fungsi hash yang digunakan adalah sha256. SHA-256 adalah varian dari keluarga Secure Hash Algorithm (SHA-2) dan menghasilkan hash 256-bit pertimbangan dipakainya fungsi hash ini adalah karena sha256 lebih aman jika dibandingkan fungsi hash lainnya.

Selain itu, algoritma kriptografi kunci publik yang akan kami gunakan adalah ElGamal. Algoritma ini telah dinilai sebagai algoritma yang cukup aman untuk memberikan tanda tangan digital. Dalam algoritma ElGamal, proses tanda tangan digital melibatkan penggunaan kunci publik dan kunci privat untuk melakukan enkripsi dan dekripsi.

Dengan menggunakan kombinasi fungsi hash SHA-256 dan algoritma kriptografi kunci publik ElGamal, kami dapat mencapai tingkat keamanan yang diharapkan dalam memberikan tanda tangan digital untuk memecahkan permasalahan ini.

B. Rancangan Solusi



Gambar 3.2.1 Rancangan solusi

terdapat dua tahap pada solusi yaitu tahap menandatangani dan tahap memverifikasi tanda tangan. Pada tahap menandatangani pesan, file tiket akan dikonversi menjadi *string* pesan. setiap file tiket akan menghasilkan informasi yang berbeda-beda bergantung pada informasi *full name*, *invoice code*, *Qty*, *seat no*, *ticket category* dan *ticket price*. sehingga setiap file tiket akan menghasilkan tanda tangan digital yang berbeda-beda. Tanda tangan tersebut juga bergantung pada kunci yang digunakan.

Berdasarkan hasil dari konversi file tiket ke string selanjutnya akan digunakan untuk menghasilkan tanda tangan digital menggunakan algoritma ElGamal. tanda tangan digital tersebut akan disimpan atau digabungkan di dalam metadata file sebelumnya sehingga nantinya dapat digunakan untuk verifikasi.

Selanjutnya tahap verifikasi digital signature yaitu pertama akan diekstrak terlebih dahulu tanda tangan digital yang terdapat pada file tiket. setelah itu akan dilakukan verifikasi tanda tangan tersebut dengan membandingkan hasil hash file tiket dengan hasil verifikasi digital signature jika sama maka file tiket tersebut valid dan tanda tangan digital tersebut sah jika tidak sama maka file tiket tersebut tidak valid.

C. Implementasi

Berikut merupakan implementasi dari rancangan solusi yang sudah dijelaskan sebelumnya.

1. Pembangkitan Kunci

   pembangkitan kunci menggunakan informasi Panjang N-bit kunci yang akan digunakan. berdasarkan panjang N kunci tersebut akan dihasilkan bilangan prima p dan generator g. Dengan parameter

tersebut dapat dihitung kunci publik dan privat yang akan digunakan.

```
def generateKey(N)
    p, g = pair(N)
    x = random(1, p-2)
    y = g^x mod p
    return p, g, x, y
```

2. Menandatangani pesan (*sign*)

Penandatanganan pesan menggunakan input pesan berupa informasi dari tiket sebagai berikut

```
Full name : AHMAD
Invoice Code : INHDA12
Qty : 4
Seat No : Free Standing
Ticket Category : MY UNIVERSE
(FESTIVAL)
Ticket Price : Rp 4.000.000
```

Penandatanganan pesan juga menggunakan p , g dan private key yang sudah di generate pada proses pembangkitan kunci. berdasarkan input tersebut akan dihasilkan output berupa r dan s yang merupakan tanda tangan digital untuk pesan tersebut. Tanda tangan digital tersebut akan disisipkan ke dalam file tiket dalam bentuk metadata.

```
def sign(p, g, x, m)
    h = hash(m)
    r = g^k mod p
    s = k^-1(h - xr) mod (p-1)
    return r,s
```

3. Memverifikasi tanda tangan (*verify*)

Pertama akan diekstrak tanda tangan digital yang terdapat pada file tiket. Hasil ekstrak tersebut adalah metadata yang berupa informasi angka prima p generator g, kunci publik y, beserta parameter tanda tangan r dan s. setelah itu akan dihitung nilai v1 dan v2 jika nilainya sama maka tanda tangan valid jika tidak maka tanda tangan tidak valid

```
def verify(p, g, y, r, s, m)
    h = hash(m)
    v1 = y^r * r^s mod p\
    v2 = g*h mod p
    return v1 = v2
```

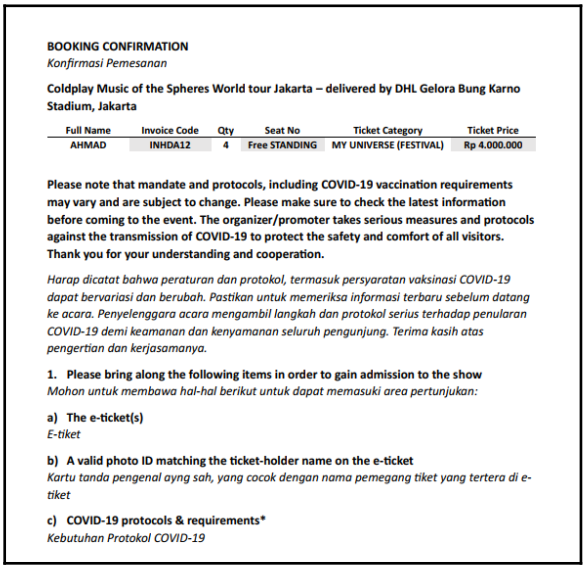
IV. Pengujian dan Pembahasan

A. *Pengujian*

Berikut akan dilakukan beberapa pengujian terhadap kasus kasus yang ada

1. Verifikasi Tiket yang Valid

Pada pengujian yang pertama akan dilakukan verifikasi terhadap tiket yang valid. Pada pengujian pertama tidak akan diubah baik isi informasi maupun tanda tangan digital. File tiket yang akan digunakan untuk pengujian adalah sebagai berikut.



BOOKING CONFIRMATION
Konfirmasi Pemesanan

Coldplay Music of the Spheres World tour Jakarta – delivered by DHL Gelora Bung Karno Stadium, Jakarta

Full Name	Invoice Code	Qty	Seat No	Ticket Category	Ticket Price
AHMAD	INHDA12	4	Free STANDING	MY UNIVERSE (FESTIVAL)	Rp 4.000.000

Please note that mandate and protocols, including COVID-19 vaccination requirements may vary and are subject to change. Please make sure to check the latest information before coming to the event. The organizer/promoter takes serious measures and protocols against the transmission of COVID-19 to protect the safety and comfort of all visitors. Thank you for your understanding and cooperation.

Harap dicatat bahwa peraturan dan protokol, termasuk persyaratan vaksinasi COVID-19 dapat bervariasi dan berubah. Pastikan untuk memeriksa informasi terbaru sebelum datang ke acara. Penyelenggara acara mengambil langkah dan protokol serius terhadap penularan COVID-19 demi keamanan dan kenyamanan seluruh pengunjung. Terima kasih atas pengertian dan kerjasamanya.

1. Please bring along the following items in order to gain admission to the show
Mohon untuk membawa hal-hal berikut untuk dapat memasuki area pertunjukan:

a) The e-ticket(s)
E-tiket

b) A valid photo ID matching the ticket-holder name on the e-ticket
Kartu tanda pengenal ayng sah, yang cocok dengan nama pemegang tiket yang tertera di e-tiket

c) COVID-19 protocols & requirements*
Kebutuhan Protokol COVID-19

Gambar 4.1.1 pengujian pertama

Berdasarkan informasi tersebut didapatkan nilai p, g, x, dan y, sebagai berikut.

```
p=216228880926584462768808534611444518
352042009845777277212315214800235259008987
g=101197764989277869368026390994455786
374799871274649891599117698527745001458487
x=154590322108476988280326563671734568
006367072025813184444839565953876904349 6
y=716157721281828488929743093184859217
018777423183865811661173822605990428290 08
```

Berdasarkan parameter tersebut didapatkan tanda tangan dengan nilai r dan s sebagai berikut.

```
r=118972894074545226369390498140574825
045089393110531013243859842373839568755788
s=168932276787343888131546227817534423
237834147861635453831057728737104691 34
```

```
8530
```

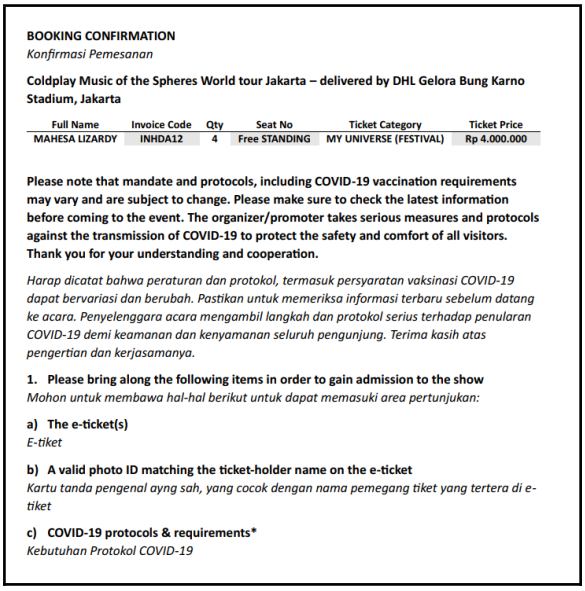
Ketika dilakukan prosedur verify untuk memverifikasi tanda tangan digital didapatkan output sebagai berikut.

```
Valid Signature = True
```

Didapatkan *valid signature* bernilai *True* yang berarti bahwa verifikasi tanda tangan digital berhasil atau tanda tangan digital valid.

2. Mengganti Informasi pada tiket yang sudah ditandatangani

Pada pengujian yang kedua akan diubah nilai dari *Full Name* berdasarkan hasil file tiket sebelumnya yang sudah valid. nilai *full name* akan diganti yang sebelumnya "AHMAD" menjadi "MAHESA LIZARDY". File tiket yang telah dimodifikasi untuk pengujian adalah sebagai berikut.



BOOKING CONFIRMATION
Konfirmasi Pemesanan

Coldplay Music of the Spheres World tour Jakarta – delivered by DHL Gelora Bung Karno Stadium, Jakarta

Full Name	Invoice Code	Qty	Seat No	Ticket Category	Ticket Price
MAHESA LIZARDY	INHDA12	4	Free STANDING	MY UNIVERSE (FESTIVAL)	Rp 4.000.000

Please note that mandate and protocols, including COVID-19 vaccination requirements may vary and are subject to change. Please make sure to check the latest information before coming to the event. The organizer/promoter takes serious measures and protocols against the transmission of COVID-19 to protect the safety and comfort of all visitors. Thank you for your understanding and cooperation.

Harap dicatat bahwa peraturan dan protokol, termasuk persyaratan vaksinasi COVID-19 dapat bervariasi dan berubah. Pastikan untuk memeriksa informasi terbaru sebelum datang ke acara. Penyelenggara acara mengambil langkah dan protokol serius terhadap penularan COVID-19 demi keamanan dan kenyamanan seluruh pengunjung. Terima kasih atas pengertian dan kerjasamanya.

1. Please bring along the following items in order to gain admission to the show
Mohon untuk membawa hal-hal berikut untuk dapat memasuki area pertunjukan:

a) The e-ticket(s)
E-tiket

b) A valid photo ID matching the ticket-holder name on the e-ticket
Kartu tanda pengenal ayng sah, yang cocok dengan nama pemegang tiket yang tertera di e-tiket

c) COVID-19 protocols & requirements*
Kebutuhan Protokol COVID-19

Gambar 4.1.2 pengujian kedua

Ketika dilakukan prosedur verify untuk memverifikasi tanda tangan digital didapatkan output sebagai berikut.

```
Valid Signature = False
```

Didapatkan *valid signature* bernilai *False* yang berarti bahwa verifikasi tanda tangan digital gagal atau tanda tangan digital tidak valid.

3. Perubahan digital signature

Pada pengujian ketiga akan dilakukan perubahan pada nilai tanda tangan digital yang terdapat pada file tiket sebagai berikut

```
r=11897289407454522636939049814057482504508939311053101324385984237383956875
4737
s=16893227678734388813154622781753442323783414786163545383105772873710469134
8328
```

Ketika dilakukan prosedur verify untuk memverifikasi tanda tangan digital didapatkan output sebagai berikut.

```
Valid Signature = False
```

Didapatkan *valid signature* bernilai *False* yang berarti bahwa verifikasi tanda tangan digital gagal atau tanda tangan digital tidak valid

B. Pembahasan

Berdasarkan pengujian yang telah dilakukan, didapatkan hasil sebagai berikut.

1. Verifikasi Tiket yang Valid

   Berdasarkan hasil tersebut didapatkan bahwa tiket verifikasi tiket menghasilkan valid signature bernilai *true*. Hal ini menandakan bahwa informasi yang terdapat di dalam file tiket merupakan informasi yang valid

2. Mengganti Informasi pada Tiket

   Berdasarkan hasil tersebut didapatkan bahwa tiket verifikasi tiket menghasilkan valid signature bernilai *false*. Hal ini menandakan bahwa informasi yang terdapat di dalam file tiket merupakan informasi yang tidak valid. Dikarenakan terdapat perubahan pada informasi *Full Name* yang sebelumnya "AHMAD" menjadi "MAHESA LIZARDY" hal ini menyebabkan verifikasi tanda tangan gagal. Sehingga dapat dipastikan jika isi file berubah meskipun hanya sedikit saja maka verifikasi tanda tangan digital akan gagal.

3. Mengganti Signature pada Tiket

   Berdasarkan hasil tersebut didapatkan bahwa tiket verifikasi tiket menghasilkan valid signature bernilai *false*. Hal ini menandakan bahwa informasi yang terdapat di dalam file tiket merupakan informasi yang tidak valid. Dikarenakan terdapat perubahan pada nilai tanda tangan digital yang terdapat pada metadata hal ini menyebabkan verifikasi tanda tangan gagal. Sehingga dapat dipastikan penggantian parameter tanda tangan digital membuat verifikasi tanda tangan digital gagal.

V. Kesimpulan dan Saran Pengembangan

Solusi implementasi tanda tangan digital telah berhasil menjaga keamanan tiket konser Coldplay dengan memenuhi aspek autentik, keaslian, dan anti penyangkalan. Hal ini dapat mengurangi resiko penipuan yang mungkin terjadi

Keamanan dari tanda tangan digital ini bergantung pada panjang kunci yang digunakan, karena pada algoritma ElGamal dengan semakin panjangnya kunci maka keamanan semakin meningkatkan namun dapat menyebabkan komputasi yang begitu lama. Sehingga perlu pertimbangan yang tepat untuk menentukan panjang kunci yang akan digunakan.

Github Link

https://github.com/lizardyy/DigitalSignatureTicket

Ucapan Terima Kasih

Penulis ingin mengucapkan terima kasih kepada Dr. Ir. Rinaldi, M.T. yang telah memberikan bimbingan dan dukungan dalam penulisan artikel ini. Serta penulis berterima kasih kepada Hokki Suwanda dan Michael Hans selaku asisten pada mata kuliah ini. Selain itu, penulis juga mengucapkan terima kasih kepada keluarga dan teman-teman yang memberikan dukungan moral selama proses penulisan artikel ini

Referensi

[1] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: 20-Algoritma ElGamal

[2] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Tanda-tangan digital (digital signature)

[3] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.

[4] National Institute of Standards and Technology (NIST). (2015). Federal Information Processing Standards Publication 180-4: Secure Hash Standard (SHS). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

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, 22 Mei 2023

Mahesa Lizardy
13520116