Penerapan Tanda Tangan Digital untuk Verifikasi Keaslian dan Integritas dari Kupon Daging Kurban Digital

Muhammad Rakha Athaya - 13520108
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520108@std.stei.itb.ac.id

***Abstrak*—Kupon pembagian daging kurban biasanya digunakan untuk menjaga ketertiban dalam pembagian daging kurban di setiap hari raya Idul Adha. Namun, terdapat beberapa masalah yang rentan muncul dalam penggunaan kupon daging kurban fisik seperti pemalsuan dan berdesak-desakkan dalam pengambilannya. Digitalisasi kupon daging kurban memberikan solusi terhadap permasalahan tersebut. Implementasi tanda tangan digital dapat memberikan lapisan keamanan yang cukup sehingga penggunaan kupon digital dapat terjaga keaslian serta integritasnya.**

Keywords—Kriptografi kunci publik, Fungsi hash, DSA, Kupon digital.

I. PENDAHULUAN

Idul Adha merupakan salah satu hari raya suci bagi umat Islam di seluruh dunia. Pada hari raya tersebut umat Islam melakukan penyembelihan hewan kurban sebagai bagian dari ibadah. Daging dari hasil penyembelihan tersebut kemudian dibagikan kepada masyarakat yang berhak mendapatkannya. Ibadah ini memiliki nilai religius sekaligus berfungsi sebagai sarana untuk mempererat hubungan sosial dan membantu golongan masyarakat yang kurang mampu. Berdasarkan World Population Review, Indonesia adalah negara dengan jumlah penduduk muslim terbesar di dunia. Sehingga, perayaan hari raya Idul Adha di Indonesia selalu berlangsung dengan meriah di setiap tahunnya.

Untuk mengatur distribusi daging kurban, biasanya digunakan kupon daging Idul Adha. Kupon ini berfungsi sebagai alat tukar agar pembagian daging kurban dilakukan secara tertib dan adil. Dengan adanya kupon daging kurban maka setiap orang yang berhak menerima dapat memperoleh bagiannya dengan mudah tanpa takut terlewat. Namun, dalam pelaksanaannya terdapat beberapa masalah yang sering kali muncul. Pemalsuan dan penyalahgunaan kupon oleh pihak yang tidak bertanggung jawab adalah salah satu masalah yang rentan terjadi. Selain itu, proses pembagian kupon daging kurban dapat juga menimbulkan masalah keributan. Pada tahun 2018, terjadi kericuhan di lokasi pembagian kupon daging kurban di Masjid Miftahul Jannah, Kota Cirebon. Warga setempat berkerumun menunggu pembagian kupon sejak pagi hari. Ketika pembagian kupon dibuka, warga berdesak-desakkan dan saling menerobos untuk mendapatkan kupon. Sejumlah anak-anak dan lansia terjepit di antara massa yang saling dorong-mendorong. Kericuhan ini membuat panitia terpaksa menghentikan pembagian kupon berkali-kali. Selain itu, sebagian warga membawa pulang lebih dari satu kupon daging dengan memanfaatkan kondisi ricuh tersebut. Kejadian tersebut menunjukkan adanya kelemahan dalam proses pembagian kupon fisik selama ini yang dapat berakibat dalam ketidakadilan dan juga risiko fisik bagi masyarakat.

Untuk mengatasi permasalahan tersebut, salah satu solusi berbasis teknologi yang dapat diterapkan adalah dengan mengubah kupon daging kurban yang berbentuk fisik menjadi kupon berbentuk digital. Kupon digital memiliki potensi untuk meningkatkan efisiensi dan mengurangi risiko penyalahgunaan. Dengan digitalisasi, distribusi kupon dapat dilakukan secara daring sehingga membuat proses pembagian lebih cepat, akurat, dan meminimalkan keperluan masyarakat untuk berkumpul secara langsung pada suatu lokasi. Namun, kupon daging kurban digital juga memiliki tantangannya tersendiri. Tantangan utama dari kupon daging kurban digital adalah kupon perlu dapat dipastikan keaslian (otentikasi) dan integritasnya. Salah satu metode yang dapat menambahkan lapisan keamanan yang dibutuhkan adalah dengan penambahan tanda tangan digital. Tanda tangan digital adalah salah satu metode kriptografi yang dapat memastikan bahwa setiap kupon yang dikeluarkan adalah asli dan tidak dapat diubah tanpa oleh pihak yang tidak berhak.

Dalam makalah ini akan dibahas mengenai implementasi tanda tangan digital pada kupon daging kurban yang berbentuk digital. Dengan penerapan tanda tangan digital ini, diharapkan dapat memberikan lapisan keamanan yang sesuai agar keaslian serta integritas dari kupon daging kurban digital dapat diverifikasi kebenarannya oleh pihak penyelenggara kurban.

II. TEORI DASAR

A. Kupon Daging Kurban

Kupon adalah surat atau karcis yang dapat ditukarkan dengan barang atau menandakan hak untuk mendapatkan atau melakukan sesuatu. Pada saat perayaan hari Idul Adha, dilakukan pemotongan hewan kurban. Daging yang didapat dari proses pemotongan ini kemudian akan dibagikan kepada

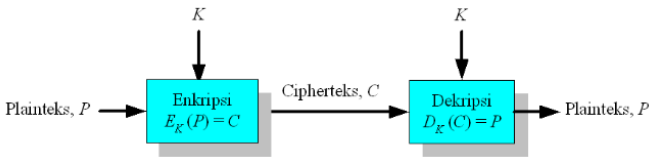
masyarakat setempat yang berhak mendapatkannya. Untuk mempermudah proses pembagian daging, panitia tempat pemotongan hewan kurban biasanya membagikan kupon daging kurban terlebih dahulu. Masyarakat yang mendapatkan kupon tersebut dapat menukarkannya dengan daging kurban setelah proses pemotongan selesai dilakukan.

Gambar 1 Kupon Daging Kurban

Pada umumnya kupon pembagian hewan kurban berisi informasi nomor penerima, lokasi pengambilan, batas waktu pengambilan, dan identitas organisasi yang menyelenggarakan pemotongan hewan kurban tersebut. Kekurangan dari kupon fisik yang selama ini digunakan adalah pembagiannya tetap dilakukan secara langsung sehingga masyarakat setempat harus datang kemungkinan berebutan kupon dikarenakan jumlahnya yang terbatas. Kupon kurban digital adalah perkembangan dari kupon fisik tradisional yang pembagiannya bisa dilakukan secara daring sehingga menghindari terjadinya rebutan dan desak-desakkan secara fisik.

B. Kritografi Kunci Publik

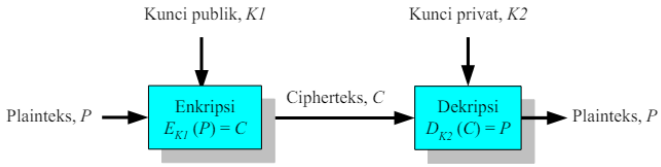
Kriptografi kunci publik atau kriptografi kunci nirsimetris adalah salah satu bagian dari kriptografi modern yang dikembangkan untuk mengatasi kekurangan dari kriptografi simetris. Konsep kriptografi kunci publik pertama kali diperkenalkan oleh Whitfield Diffie dan Martin E. Hellman pada tahun 1976 lewat makalahnya yang berjudul “New Directions in Cryptography”. Pada tahun-tahun sebelumnya, hanya diketahui sistem kriptografi kunci simetris di mana pengirim dan penerima pesan keduanya memiliki kunci rahasia yang sama untuk proses enkripsi dan dekripsi.



Gambar 2 Proses Kriptografi Kunci Simetris

Kelebihan dari sistem ini adalah proses enkripsi dan dekripsi membutuhkan waktu yang singkat serta panjang kunci rahasia yang relatif lebih pendek. Keaslian dari pesan juga dapat langsung diketahui karena hanya pengirim dan penerima yang memiliki kunci rahasia. Namun, kelemahan dari sistem kriptografi ini adalah kunci rahasia harus dikirim melalui saluran yang aman dan terpercaya untuk menghindari pihak ketiga mengetahui nilai dari kunci rahasia tersebut. Pihak pengirim dan penerima juga harus selalu menjaga kerahasiaan dari kunci tersebut, sehingga nilai kunci yang digunakan dalam komunikasi perlu diganti secara rutin.

Sistem kriptografi kunci publik memungkinkan pihak pengirim dan penerima untuk berkomunikasi melalui saluran yang tidak aman. Hal tersebut dicapai dengan menggunakan dua jenis kunci rahasia, yaitu kunci privat dan kunci publik. Kunci privat digunakan untuk mendekripsi pesan sementara kunci publik digunakan untuk mengenkripsi pesan. Kedua pihak memiliki pasangan kuncinya masing-masing, dengan kunci publik dapat diumumkan secara bebas sementara kunci privat hanya diketahui oleh pemiliknya.



Gambar 3 Proses Kriptografi Kunci Publik

Keuntungan dari sistem ini adalah kunci privat tidak perlu dikirimkan sehingga tidak diperlukan adanya saluran terpercaya untuk berkomunikasi. Pasangan kunci yang dimiliki setiap pihak juga tidak perlu sering dirubah. Sifat dari kriptografi kunci publik ini juga dapat dimanfaatkan dalam pengiriman kunci rahasia dalam kriptografi kunci simetris. Sementara itu, kelemahan dari kriptografi kunci publik adalah proses enkripsi dan enkripsi yang lebih lambat, ukuran cipherteks yang lebih besar dari plainteks, ukuran kunci yang relatif besar, serta tidak dapat mengetahui keaslian pengirim karena kunci publik diketahui secara umum.

Algoritma dalam kriptografi kunci publik dapat bekerja dengan dasar persoalan integer klasik yang sangat sulit dipecahkan, sehingga secara komputasi hampir tidak mungkin mengetahui nilai kunci privat dari nilai kunci publik. Beberapa persoalan tersebut meliputi:

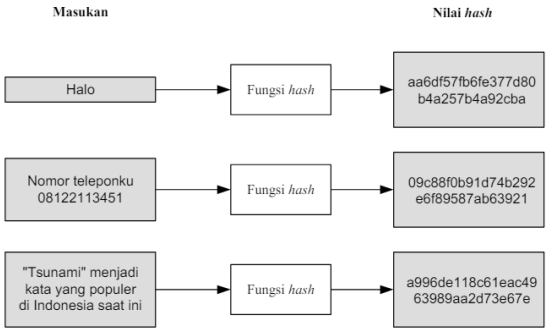
1) Pemfaktoran.
2) Logaritma diskrit.
3) *Elliptic Curve Discrete Logarithm Problem*.
4) Knapsack Problem.
5) Persamaan diophantine.

Kriptografi kunci publik sebagai bagian dari kriptografi modern memiliki aplikasi yang luas. Beberapa aplikasi dari kriptograsi kunci publik adalah dalam enkripsi dan dekripsi pesan, pertukaran kunci, serta dalam implementasi tanda tangan digital.

C. Hash

Fungsi *hash* adalah fungsi yang dapat mengkompresi sebuah pesan *M* dengan ukuran sembarang menjadi sebuah *string h* dengan ukuran tetap. Hasil dari fungsi *hash* disebut sebagai *message digest* atau nilai *hash*. Properti utama dari fungsi *hash* adalah hasilnya bersifat *irreversible* yang berarti *message digest* tidak dapat dikembalikan menjadi pesan semula. Fungsi *hash* berbeda dengan fungsi enkripsi karena fungsi *hash* tidak memerlukan kunci serta nilai *hash* tidak dapat dikembalikan menjadi pesan semua (tidak dapat melakukan dekripsi). Fungsi *hash* yang aman secara kriptografis adalah fungsi *hash* yang

tidak memiliki kolisi, yaitu kondisi dua pesan yang berbeda memiliki nilai *hash* yang sama.



Gambar 4 Gambaran Fungsi Hash

Fungsi *hash* memiliki beberapa sifat, yaitu:

1) *Collision resistance*; sangat sulit untuk menemukan dua pesan sembarang dengan nilai *hash* yang sama.
2) *Preimage resistance*; sulit untuk menemukan nilai pesan dari nilai *hash*-nya.
3) *Second preimage resistance*; sulit menemukan nilai pesan yang menghasilkan nilai *hash* yang sama dengan nilai *hash* dari pesan lain yang sudah diketahui.

Fungsi *hash* juga memiliki banyak aplikasi, meliputi:

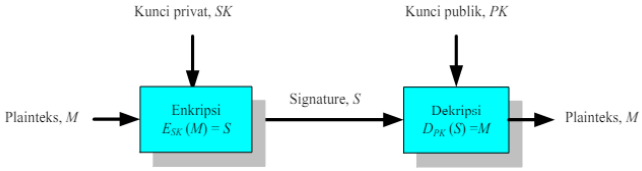
1) Menjaga integritas pesan.
2) Menghemat waktu pengiriman dalam verifikasi.
3) Menyamakan panjang data yang berbeda-beda.

D. *Tanda Tangan Digital*

Tanda tangan digital merupakan sebuah nilai kriptografis yang ditentukan oleh kunci dan isi pesan yang diberikan tanda tangan. Tanda tangan digital dikembangkan sebagai versi digital dari tanda tangan biasa yang digunakan pada dokumen dan data digital. Tanda tangan digital digunakan untuk otentikasi, nir-penyangkalan, dan menjadi integritas. Beberapa persyaratan yang harus dimiliki tanda tangan digital adalah:

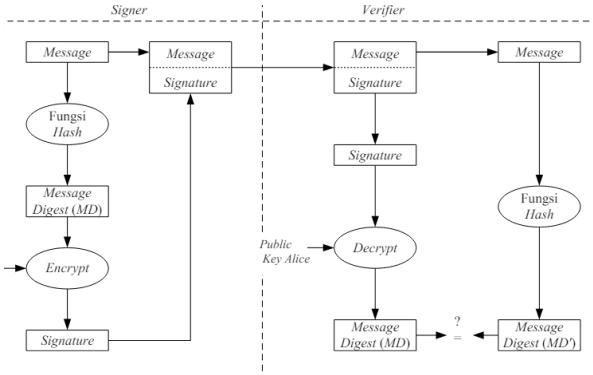
1) Proses pembangkitan tanda tangan digital harus relatif mudah untuk dilakukan.
2) Proses pengenalan dan verifikasi tanda tangan digital harus relatif mudah untuk dilakukan.
3) Tanda tangan digital harus berupa rangkaian bit yang ditentukan oleh informasi unik berupa kunci dan pesan yang diberikan tanda tangan.
4) Pemalsuan tanda tangan digital harus hampir tidak mungkin dilakukan secara komputasi.

Terdapat dua proses yang dilakukan dalam memberikan tanda tangan digital, yaitu menandatangani pesan (*signing*) dan memverifikasi pesan (*verification*). Dalam implementasi tanda tangan digital terdapat dua cara yang dapat dilakukan. Cara pertama adalah dengan mengenkripsi keseluruhan pesan. Pada kriptografi kunci simetris, mengenkripsi keseluruhan pesan dapat menjadi solusi dalam otentikasi pengirim pesan karena hanya pengirim dan penerima yang memiliki kunci rahasia. Namun, penyangkalan masih dapat dilakukan karena tidak ada bukti pihak mana yang melakukan enkripsi. Sehingga, untuk tanda tangan digital menggunakan kriptografi simetris diperlukan adanya pihak ketiga yang dipercaya (*arbitrase*).



Gambar 5 Proses Kriptografi Kunci Publik untuk Tanda Tangan Digital

Pada kriptografi kunci publik, proses tanda tangan digital dapat dilakukan dengan menukar penggun aan kunci privat dan kunci publik. Proses enkripsi dilakukan dengan menggunakan kunci privat sementara proses dekripsi menggunakan kunci publik. Penyangkalan tidak dapat dilakukan karena hanya pihak yang memegang kunci privat yang dapat mengenkripsi pesan sementara semua orang dapat memverifikasinya dengan kunci publik yang diketahui secara umum. Dengan demikian penggunaan kriptografi kunci publik untuk tanda tangan digital lebih efektif dan tidak memerlukan pihak ketiga.



Gambar 6 Skema Tanda Tangan Digital Kombinasi Kriptografi Kunci Publik dengan Fungsi Hash

Cara kedua dari implementasi tanda tangan digital adalah dengan menggabungkan kriptografi kunci publik dengan fungsi *hash*. Cara kedua ini dilakukan ketika kerahasiaan dari isi pesan tidak diperlukan, sehingga hanya diperlukan otentikasi pengirim dan integritas pesannya saja. Hal ini berbeda dengan cara pertama yang mengenkripsi keseluruhan pesan karena isi pesan bersifat rahasia. Berikut adalah tahapan secara umum dalam tanda tangan digital dengan menggunakan kombinasi kriptografi kunci publik dan fungsi *hash*:

1) Fungsi *hash* digunakan untuk menghasilkan *message digest* dari isi pesan yang akan diberikan tanda tangan.
2) *Message digest* tersebut dienkripsi menggunakan algoritma kriptografi kunci publik dengan kunci privat milik pengirim. Hasil dari enkripsi *message digest* disebut sebagai *signature*.
3) *Signature* ditempelkan pada pesan asli. Gabungan dari pesan asli dan *signature* inilah yang merupakan pesan yang telah ditandatangani.
4) Penerima pesan memulai proses verifikasi tanda tangan digital dengan memisahkan *signature* dari isi pesan. Penerima kemudian mendekripsi *signature* menggunakan kunci publik milik pengirim untuk mendapatkan *message digest* awal.

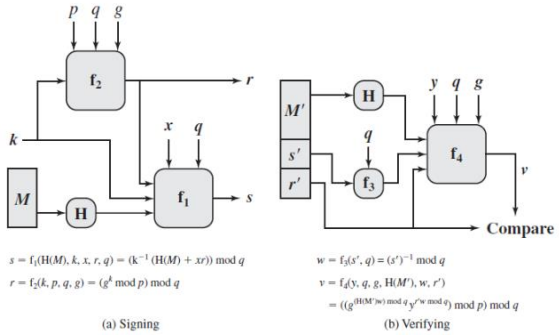
5) Penerima membandingkan nilai *message digest* yang didapat dari proses dekripsi *signature* dengan *message digest* yang didapat dari memasukkan isi pesan yang diterima ke fungsi *hash*. Apabila keduanya sama, maka tanda tangan digital berhasil diverifikasi.

E. *Digital Signature Algorithm*

Digital Signature Agorithm (DSA) adalah sebuah algoritma kriptografi kunci publik yang digunakan secara khusus untuk tanda tangan digital. DSA merupakan bagian dari *Digital Signature Standard* (DSS) yang diresmikan pada tahun 1991 oleh The National Institute of Standard and Technology (NIST) sebagai bakuan untuk proses tanda tangan digital. DSA merupakan pengembangan dari algoritma ElGamal dan menggunakan sepasang kunci privat dan kunci publik seperti algoritma kriptografi kunci publik pada umumnya.

Parameter DSA terdiri dari parameter publik, kunci privat, kunci publik, dan pesan sebagai berikut:

1) Parameter publik bilangan prima *p*.
2) Parameter publik bilangan prima *q* dengan
$$(p-1)\ mod\ q = 0$$
3) Parameter publik *g* dengan
$$g = h^{(p-1)/q}\ mod\ p$$
$$h < p-1$$
$$h^{(p-1)/q}\ mod\ p > 1$$
4) Kunci privat *x*, berupa bilangan bulat kurang dari *q*.
5) Kunci publik *y* dengan
$$y = g^x\ mod\ p$$
6) Isi pesan *m* yang akan diberikan tanda tangan.



Gambar 7 Proses DSA

Terdapat 3 proses yang dilakukan dalam penggunaan DSA untuk tanda tangan digital, yaitu:

1) *Pembangkitan Pasangan Kunci*
Dalam proses ini akan dibangkitkan pasangan kunci privat dan kunci publik menggunakan parameter *p*, *q*, dan *g* yang telah ditentukan.
2) *Pembangkitan Tanda Tangan Digital (Signing)*
Signing dilakukan dengan menghitung *message digest* dari pesan dengan menggunakan fungsi hash SHA-1. Lalu, tentukan bilangan acak *k*, dengan $0 < k < q$. *Signature* adalah bilangan *r* dan *s* yang didapat dengan rumus sebagai berikut menggunakan kunci privat *x*. Setelah itu, pesan dikirim dengan *signature* (*r*,*s*).

$$r = (g^k\ mod\ p)\ mod\ q$$

$$s = (k^{-1}\ (message\ digest + x \cdot r))\ mod\ q$$

3) *Verifikasi Tanda Tangan Digital*
Verifikasi dilakukan dengan pertama menghitung *message digest* dari isi pesan menggunakan fungsi hash SHA-1. Kemudian, dilakukan pemrosesan *signature* (v) dilakukan dengan rumus sebagai berikut menggunakan kunci publik *y*. Jika nilai *v* sama dengan nilai *r*, maka hasil dari verifikasi tanda tangan digital dinyatakan sah.

$$w = s^{-1}\ mod\ q$$
$$u_1 = (message\ digest \cdot w)\ mod\ q$$
$$u_2 = (r \cdot w)\ mod\ q$$
$$v = ((g^{u1} \cdot y^{u2})\ mod\ p)\ mod\ q$$

III. IMPLEMENTASI

A. *Desain Implementasi Program*

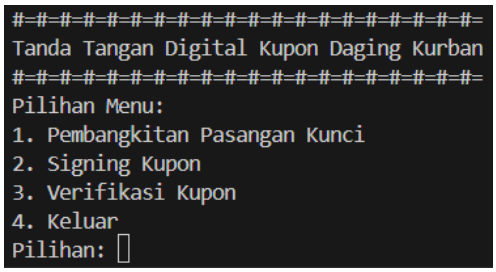
Program yang akan dibuat adalah sebuah program sederhana yang dapat memberikan tanda tangan digital pada file kupon daging kurban digital serta memverifikasi keasliannya. Program dikembangkan dengan bahasa pemrograman Python dan dapat dijalankan secara lokal melalui CLI komputer. File kupon daging kurban digital yang dapat diproses oleh program memiliki format pdf. Proses pembangkitan tanda tangan digital menggunakan kombinasi kriptografi kunci publik dan fungsi hash. Cara ini dipilih karena isi dari file kupon tersebut tidak bersifat rahasia dan justru perlu dapat dibaca oleh penerima kupon daging kurban digital. Algoritma yang digunakan mengikuti *Digital Signature Standard* (DSS), yaitu *Digital Signature Agorithm* (DSA). Isi pesan yang akan digunakan dalam DSA adalah isi teks dari file pdf kupon daging kurban. Kemudian, nilai signature akan disimpan ke dalam metadata dari file tersebut. Hal ini dipilih untuk menghindari verifikasi tanda tangan gagal apabila nama file berubah dan juga tidak mengubah tampilan dari kupon secara visual. Berikut adalah alur dari proses yang akan dilakukan dalam proses pemberian tanda tangan digital dan verifikasinya menggunakan progam:

1) Pertama-tama pengguna yang berperan sebagai panitia penyelenggara pembagian daging kurban membangkitkan pasangan kunci privat dan kunci publik menggunakan program. Pasangan kunci tersebut kemudian harus dicatat dan disimpan oleh pihak penyelenggara.
2) Untuk membuat sebuah kupon daging kurban yang sah, pengguna harus memberikan tanda tangan digital kepada file kupon tersebut sebelum dikirimkan ke penerima secara daring. Pemberian tanda tangan digital dilakukan dengan memasukkan file pdf kupon dan nilai kunci privat ke dalam program. Program akan mengambil isi teks dari file untuk dijadikan sebagai parameter isi pesan *m* dalam proses DSA. *Signature* yang dihasilkan kemudian dimasukkan ke dalam metadata file kupon. File yang dihasilkan adalah kupon daging kurban digital yang sudah ditandatangani dan dapat dikirimkan ke penerima yang sesuai.
3) Pada hari penukaran kupon, pihak penyelenggara dapat memverifikasi keaslian dari kupon daging kurban

digital yang diterima kembali dengan memasukkan file kupon yang diterima dan nilai kunci publik ke dalam program.

4) Program akan mengambil nilai *signature* dan isi teks dari file yang akan digunakan dalam proses verifikasi DSA. Jika hasil pemrosesan *signature* sama dengan nilai komponen *r* dari *signature*, maka tanda tangan dinyatakan valid. Jika tidak, maka kupon telah mengalami modifikasi atau kupon tersebut tidak berasal dari penyelenggara yang sah.

Implementasi dari program ini menggunakan *library PyPDF2* untuk memproses file pdf dan *library cryptography* untuk memproses DSA dan fungsi *hash*. Fungsi *hash* yang digunakan adalah SHA-256 yang merupakan peningkatan dari SHA-1 yang biasanya digunakan pada DSA. Program juga memiliki menu utama untuk memudahkan pengguna dalam menggunakannya. Berikut adalah tampilan dari menu utama program.



Gambar 8 Menu Utama Program

IV. PEMBAHASAN

A. *Uji Coba Program*

Eksperimen dilakukan untuk menguji fungsionalitas dari setiap fitur program. File kupon daging kurban yang akan digunakan dalam eksperimen adalah file "kupon.pdf".

Gambar 9 File kupon.pdf

Pada kasus pertama, dilakukan uji coba pada kondisi normal. Pengguna pertama-tama membangkitkan pasangan kunci privat dan publik dengan mengakses menu 1. Berikut adalah pasangan kunci yang dihasilkan.

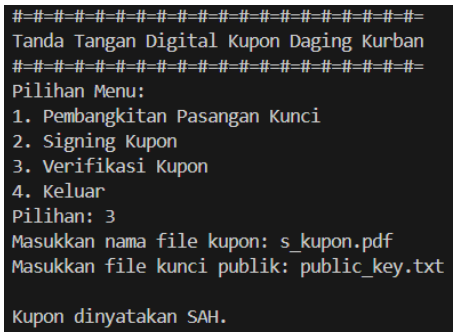
```
Private Key:

MIICZAIBADCCAjkGByqGSM44BAEwggIsAoIBAQCJmz+K/NzljU8MP1Q
pvJqWniyMCIsSeCooFCSoPOdPmA5GzHWvvmavbf9u/iurPG/S/56rId
/sP/Dg1n9rEotN7Kl+XLTS2maPf7PiySfktcSX3lhWMjd0o41Tanot2
SsOYbSpEoLUTBBV2TpKBazVudUfHG+x0DaOGO/7MmBrx00tUeg8WKgg
lOxesV93Jvrk076w+x6gImzgOE+e8Aj71Z0sGgmJiD+/I5TDP3k9ywo
JiMBvGViDibaEktJO4Q9mu8oiu0FeON6eRSd0do5426PbzOwJZH5KCU
Sootgn/3CAOyeuD4VLwMDy8WV+WbuKywNfKJJd4CuX7Qn05t5AiEAub
Nc5q1dwfanOtSiLR/JC8QsQm3Dw1/RCZFwfHaEgqcCggEABf18aszXa
SLE7FqLyslkOf2VBfCxcsP24BiiMj8Ab06hbQOylAiqhTx5kcpWgvP8
MIxpkeZzR0AwwfiLiVfNAt0aZChEafEFnBQWNSnVbhPigJYr1OPR0eJ
+tl74Yiwh3Z9NrtwGfkankUu5D93zwV+dBfunVnFf5z2TntEzFeZMse
0TUuSbhzTmbcPEIIsdUS2f0KnM7Te6DZ1yYHKLYEBnXZfyoEH5iQ8BZ
jhGkNtIeQ4Q2RFbJSot39rscpavd5xofPryVEa5b0vFNmYFkkVFNToZ
cKmi02LBKpMKe0ryraak5GU/RrFXMIeqFFtxt91upFoJ4ITX5v+NCEV
KwQiAiAobiDKfwoM783BeaLFBr2KOHYm8ciuiFfrmck7A/V9Hw==

Public Key:

MIIDRjCCAjkGByqGSM44BAEwggIsAoIBAQCJmz+K/NzljU8MP1QpvJq
WniyMCIsSeCooFCSoPOdPmA5GzHWvvmavbf9u/iurPG/S/56rId/sP/
Dg1n9rEotN7Kl+XLTS2maPf7PiySfktcSX3lhWMjd0o41Tanot2SsOY
bSpEoLUTBBV2TpKBazVudUfHG+x0DaOGO/7MmBrx00tUeg8WKgglOxe
sV93Jvrk076w+x6gImzgOE+e8Aj71Z0sGgmJiD+/I5TDP3k9ywoJiMB
vGViDibaEktJO4Q9mu8oiu0FeON6eRSd0do5426PbzOwJZH5KCUSoot
gn/3CAOyeuD4VLwMDy8WV+WbuKywNfKJJd4CuX7Qn05t5AiEAubNc5q
1dwfanOtSiLR/JC8QsQm3Dw1/RCZFwfHaEgqcCggEABf18aszXaSLE7
FqLyslkOf2VBfCxcsP24BiiMj8Ab06hbQOylAiqhTx5kcpWgvP8MIxp
keZzR0AwwfiLiVfNAt0aZChEafEFnBQWNSnVbhPigJYr1OPR0eJ+tl7
4Yiwh3Z9NrtwGfkankUu5D93zwV+dBfunVnFf5z2TntEzFeZMse0TUu
SbhzTmbcPEIIsdUS2f0KnM7Te6DZ1yYHKLYEBnXZfyoEH5iQ8BZjhGk
NtIeQ4Q2RFbJSot39rscpavd5xofPryVEa5b0vFNmYFkkVFNToZcKmi
02LBKpMKe0ryraak5GU/RrFXMIeqFFtxt91upFoJ4ITX5v+NCEVKwOC
AQUAAoIBAAfpxBifTWyIdA1r8quM3hZauakHXONhFz+O4wRMdLGgsRl
cKoLNG9QKpp2T9pzMlTlFjVjAD6QZWleLIxaEJvpJgK21Op0jA099FL
/qwY3kfSWpsKWNGbEai2xWviniere/PWU8QyUVFdsnWdNmrwzk9SwkB
hVzI6qVjXXYAlD1fB4Hg2Fv0/lE9hqFfpDyLM9z/KjaRQ66xwd9n2y4
Ut7eB0OUrELuOPNiDVs6ZgouKlCrUYuKZtifmxmBYgufWvrjD5EZhOe
gZFcMYi1g+pLfmquMEf2fW4rplx0WNCUcaxE24Kdsqapzkft24BDHx4
lv0IZNHMKFjT2HRfGMY0=
```

Selanjutnya dilakukan proses signing pada file kupon.pdf dengan menggunakan kunci privat yang sesuai melalui menu 2. File yang dihasilkan berupa s_kupon.pdf yang sudah memiliki signature di dalam metadatanya. Proses verifikasi terhadap file s_kupon.pdf dilakukan dengan menggunakan kunci publik yang sesuai melalu menu 3.



Gambar 10 Hasil Verifikasi File s_kupon.pdf

Pada kasus berikutnya, dilakukan uji coba pada kondisi kupon yang sudah ditandatangani dirubah isi teksnya. Pada kasus ini dilakukan perubahan nomor kupon yang tertera pada file s_kupon.pdf yang dihasilkan pada uji coba sebelumnya. Proses verifikasi kembali dilakukan melalui menu 3 dengan menggunakan kunci publik sama.

Gambar 11 File s_kupon_edit.pdf

```
#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=
Tanda Tangan Digital Kupon Daging Kurban
#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=
Pilihan Menu:
1. Pembangkitan Pasangan Kunci
2. Signing Kupon
3. Verifikasi Kupon
4. Keluar
Pilihan: 3
Masukkan nama file kupon: s_kupon_edit.pdf
Masukkan file kunci publik: public_key.txt
Verification failed:

Kupon dinyatakan TIDAK SAH.
```

Gambar 12 Hasil Verifikasi File s_kupon_edit.pdf

Pada kasus terakhir, dilakukan uji coba pada kondisi kupon dengan tampilan yang sama dengan kupon sah namun tidak bertandatangan. Pada kasus ini dilakukan proses verifikasi terhadap file kupon.pdf yang tidak memiliki tanda tangan melalui menu 3 dengan menggunakan kunci publik sama.

```
#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=
Tanda Tangan Digital Kupon Daging Kurban
#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=#=
Pilihan Menu:
1. Pembangkitan Pasangan Kunci
2. Signing Kupon
3. Verifikasi Kupon
4. Keluar
Pilihan: 3
Masukkan nama file kupon: kupon.pdf
Masukkan file kunci publik: public_key.txt
File kupon tidak bertanda tangan.
```

Gambar 13 Hasil Verifikasi File kupon.pdf

B. *Analisis*

Fungsionalitas program dalam memberikan tanda tangan digital kepada kupon daging kurban digital serta memverifikasi kebenarannya telah berjalan dengan baik. Pada kasus pertama, proses *signing* dan verifikasi terhadapa file kupon yang bertanda tangan berhasil dilakukan. Pada kasus kedua, verifikasi terhadap file kupon bertandatangan yang dirubah isi teksnya berhasil menunjukkan bahwa kupon tersebut tidak sah. Pada kasus terakhir, program juga berhasil menunjukkan bahwa file kupon tidak memiliki *signature* sehingga bukan merupakan file kupon daging kurban yang dibagikan oleh penyelenggara. Hasil uji coba pada ketiga kasus tersebut menunjukkan bahwa pemberian tanda tangan digital dapat menjaga keaslian serta integritas dari kupon daging kurban digital.

V. KESIMPULAN DAN SARAN

A. *Kesimpulan*

Implementasi tanda tangan digital menggunakan DSA dan fungsi hash SHA-256 pada kupon daging kurban digital dapat memberikan lapisan keamanan yang cukup untuk menjaga keaslian serta integrasinya. Pihak penyelenggara pembagian daging kurban dapat membagikan kupon digital yang telah diberikan tanda tangan kepada para penerima secara daring. Pada hari pembagian, verifikasi file kupon dapat dilakukan dengan mudah melalui program yang diusulkan serta mampu menangkap adanya upaya penyalahgunaan kupon seperti mengubah isi kupon ataupun pembuatan kupon sendiri. Hal ini menjadikan kupon daging kurban digital aman untuk dijadikan pengganti dari kupon daging kurban fisik.

B. *Saran*

Implementasi program dalam makalah ini masih berfokus pada kasus kupon digital dengan format pdf saja. Pengembangan untuk menerima berbagai jenis format file lain dapat dilakukan untuk meningkatkan fleksibilitas dari penggunaan program. Selain itu dapat juga dikembangkan sistem untuk melakukan verifikasi banyak kupon secara langsung untuk mempercepat proses penukaran daging kurban di lokasi.

VI. UCAPAN TERIMA KASIH

Penulis mengucapkan rasa syukur kepada Allah SWT. atas segala rahmat dan karunia-Nya yang telah memungkinkan penulis untuk menyelesaikan makalah yang berjudul "Penerapan Tanda Tangan Digital untuk Verifikasi Keaslian dan Integritas dari Kupon Daging Kurban Digital" ini. Penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada Bapak Rinaldi Munir, selaku dosen mata kuliah IF4020 Kriptografi, atas segala bimbingan dan ilmu yang telah diberikan. Ucapan terima kasih juga penulis sampaikan kepada orang tua dan teman-teman penulis yang selalu memberikan dukungan dan semangat selama proses perkuliahan.

REFERENSI

[1] Munir, Rinaldi. 2024. *Kriptografi Kunci-Publik*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/17-Kriptografi-Kunci-Publik-2024.pdf

[2] Munir, Rinaldi. 2024. *Fungsi Hash*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/24-Fungsi-hash-2024.pdf

[3] Munir, Rinaldi. 2024. *Tanda-tangan Digital*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/29-Tanda-tangan-digital-2024.pdf

[4] Munir, Rinaldi. 2024. *Digital Signature Standard (DSS)*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/31-DSS-2024.pdf

[5] *Muslim Population by Country 2024*. World Population Review. 2024. Diakses pada 21 Juni 2024. https://worldpopulationreview.com/country-rankings/muslim-population-by-country

[6] *Pembagian Daging Kurban Ricuh, Warga Berdesakan Rebutan Kupon*. Sindo News. 2018. Diakses pada 21 Juni 2024. https://daerah.sindonews.com/berita/1332312/21/pembagian-daging-kurban-ricuh-warga-berdesakan-rebutan-kupon

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, 23 Juni 2024

Muhammad Rakha Athaya
13520108