Implementasi Tanda Tangan Digital pada Struk Belanja di Supermarket

18220009 Fatih Darielma Gaizta
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10, Bandung
18220009@std.stei.itb.ac.id

***Abstract*—Tanda tangan digital adalah metode otentikasi elektronik yang menggunakan kunci kriptografi untuk memastikan integritas dan keaslian dokumen digital. Dalam konteks struk belanja, tanda tangan digital digunakan untuk memverifikasi keaslian dan keabsahan transaksi, serta melindungi dokumen dari pemalsuan atau manipulasi. Tanda tangan digital pada struk belanja dapat diimplementasikan dengan mengintegrasikan program penanda tangan digital dan sertifikat digital dengan sistem kasir. Penggunaan tanda tangan digital membawa beberapa tantangan atau masalah yang mungkin dihadapi, seperti kebijakan keamanan dan privasi data, kesadaran pengguna, serta kepatuhan hukum terkait dokumen digital. Namun, implementasi tanda tangan digital pada struk belanja di supermarket dapat memberikan manfaat besar dalam meningkatkan efisiensi dan keamanan transaksi.**

Keywords—tanda tangan digital; RSA; hash; digital; dokumen; struk; transaksi; verifikasi; otentik

I. Pendahuluan

Dalam dunia bisnis yang semakin terhubung secara digital, supermarket menjadi salah satu sektor yang mengadopsi teknologi untuk meningkatkan pengalaman belanja pelanggan. Namun, meskipun transaksi elektronik telah menjadi standar dalam lingkungan ritel, masih terdapat beberapa kelemahan dalam hal otentikasi dan keamanan dokumen digital, terutama struk belanja. Struk belanja memainkan peran penting dalam memberikan bukti transaksi kepada pelanggan sehingga penting untuk memastikan integritas dan keaslian dokumen tersebut. Dalam upaya mengatasi tantangan ini, penelitian ini bertujuan untuk mengeksplorasi dan menerapkan tanda tangan digital pada struk belanja di supermarket. Dengan memanfaatkan teknologi kriptografi modern, tanda tangan digital dapat memberikan solusi yang aman dan efisien untuk memverifikasi keaslian dan integritas dokumen digital. Melalui penelitian ini, diharapkan dapat ditemukan solusi yang efektif untuk meningkatkan keamanan transaksi dan memperkuat kepercayaan pelanggan dalam penggunaan struk belanja elektronik di supermarket.

II. Dasar Teori

A. Algoritma RSA

Algoritma RSA merupakan algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya. Algoritma ini dibuat oleh tiga peneliti dari MIT, yaitu Ronald Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan bulat yang besar menjadi faktor-faktor prima. Kunci untuk enkripsi dan dekripsi pada algoritma RSA dibangkitkan dengan memilih dua bilangan prima p dan q di mana p tidak sama dengan q. Berikut merupakan proses pembangkitan sepasang kunci enkripsi dan dekripsi pada algoritma RSA.

1. Pilih dua bilangan prima p dan q
2. Hitung n, di mana $n = p \times q$
3. Hitung $\phi(n)$, di mana $\phi(n) = (p - 1) \times (q - 1)$
4. Pilih satu bilangan acak yang relatif prima terhadap $\phi(n)$ untuk dijadikan kunci publik, misal e
5. Hitung kunci d untuk dekripsi dengan persamaan $d = \frac{1+k\phi(n)}{e}$, di mana k adalah anggota himpunan bilangan asli yang membuat d bernilai bulat

Setelah itu, pesan m dapat dienkripsi menjadi ciphertext c dengan rumus $c = m^e \pmod n$ dan didekripsi kembali menjadi pesan m dengan rumus $m = c^d \pmod n$.

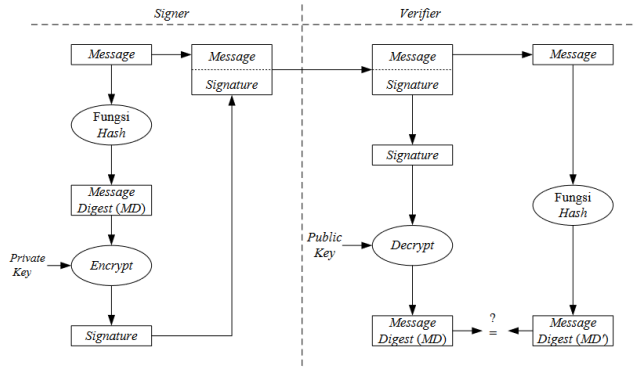
Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan bulat n, yaitu faktor-faktor prima p dan q. Oleh karena itu, algoritma RSA akan lebih baik jika nilai dari bilangan prima p dan q memiliki panjang lebih dari 100 digit sehingga waktu komputasi untuk mencari faktor-faktor prima tersebut membutuhkan waktu lebih dari 4 miliar tahun.

B. Tanda Tangan Digital

Tanda tangan digital adalah metode otentikasi elektronik yang menggunakan kunci kriptografi untuk memastikan integritas dan keaslian dokumen digital. Tanda tangan seseorang pada suatu dokumen cetak akan selalu sama, apapun isi dokumennya, sedangkan tanda tangan digital selalu berbeda-beda antara satu pesan dengan pesan lain dan antara satu kunci dengan kunci yang lain. Tanda tangan digital sangat bergantung kepada isi dokumen sehingga apabila dokumennya berubah, tanda tangan juga akan ikut berubah.

Membuat tanda tangan digital pada sebuah dokumen melibatkan fungsi hash dan algoritma kriptografi untuk mengenkripsi dan mendekripsi pesan. Algoritma kriptografi yang digunakan untuk membuat tanda tangan digital adalah algoritma RSA karena sifat dari persamaan enkripsi dan dekripsi yang bisa dipertukarkan. Dalam hal ini, kunci publik

dalam algoritma RSA akan digunakan untuk verifikasi tanda tangan digital, sedangkan kunci private-nya akan digunakan untuk menandatangani dokumen. Berikut merupakan skema pengiriman pesan dengan tanda tangan digital dan pemverifikasian pesan. Kunci publik dan private yang digunakan dalam skema ini adalah kunci milik pengirim.



Gambar 1. Skema pengiriman dan pemverifikasian pesan.

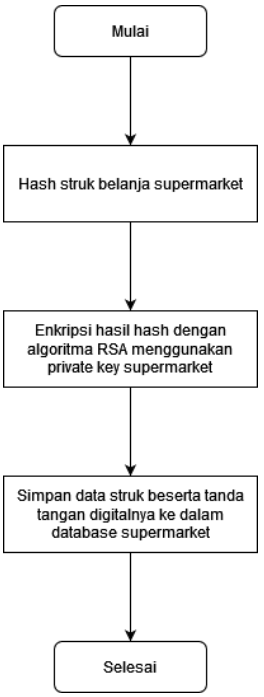
C. Hash

Fungsi hash adalah fungsi yang mengkompresi pesan berukuran sembarang menjadi string dengan ukuran tertentu. Output berupa string yang dihasilkan dari fungsi hash disebut message-digest. Salah satu ciri khas dari message-digest adalah sifatnya yang irreversible, yaitu tidak bisa dikembalikan menjadi pesan semula. Selain itu terdapat juga beberapa sifat dari fungsi hash yang di antaranya ialah sebagai berikut.

- Collision resistance, yaitu sangat sulit menemukan dua input a dan b yang memenuhi H(a) = H(b)
- Preimage resistance, yaitu untuk sembarang message-digest y, sulit menemukan input a yang memenuhi H(a) = y
- Second preimage resistance, yaitu untuk input a dan message-digest y = H(a), sulit menemukan input lain b yang memenuhi H(b) = y

III. RANCANGAN DAN IMPLEMENTASI

Cara kerja dari implementasi tanda tangan digital pada struk belanja di supermarket membutuhkan sebuah program untuk dipasang pada komputer kasir. Ketika harga barang-barang sudah selesai di-input untuk struk belanja, sebelum struk belanja tersebut di cetak, isi konten di-hash lalu dienkripsi dengan algoritma RSA sehingga menghasilkan message-digest. Tanda tangan supermarket dapat diverifikasi, baik oleh pembeli maupun pemilik supermarket. Berikut merupakan flowchart untuk proses penandatanganan dan verifikasi struk belanja di supermarket.



Gambar 2. Flowchart proses penandatanganan struk belanja.

Gambar 3. Flowchart proses verifikasi struk belanja.

Implementasi pada penelitian ini akan menggunakan sebuah prototype yang berbentuk program yang mensimulasikan proses penandatanganan dan pemverifikasian tanda tangan digital pada struk belanja sesuai dengan flowchart yang ada pada Gambar 2 dan Gambar 3.

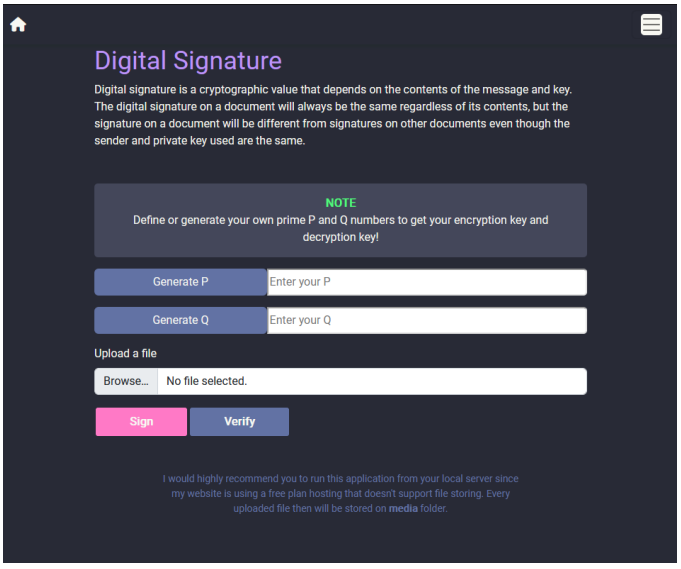
A. Implementasi

Implementasi tanda tangan digital pada struk belanja disimulasikan dengan menggunakan data dummy dan bahasa pemrograman Python. Berikut merupakan modul yang berisi potongan kode dari fungsi-fungsi untuk membuat tanda tangan digital.

```
'''
Digital Signature with RSA
[1] Hash message M: H(M) = h
[2] Encrypt hashed message with private
key: S = E_sk(h) mod n
[3] Output M + S, so that receiver can
see the message and the signature

Verify Message
[1] Hash message M: H(M) = h
[2] Decrypt encrypted hashed message (S)
with sender's public key: h' = D_pk(S)
mod n
[3] Compare h with h'
      If both are the same, then the
message M is authentic (not modified).
      Else, it's not authentic.

Generate RSA Key
[1] Pick two prime number p and q
[2] Calculate n: n = p * q
[3] Calculate phi(n): phi(n) = (p-1) *
(q-1)
[4] Pick a random whole number e that is
prime relative to phi(n)
[5] Calculate decryption key d with
Euclidean algorithm :') until we have d
is a whole number
      d = (1 + (k * phi(n))) / e
'''

import math
import hashlib


'''
Read File as Bytes
'''
def read_file_in_bytes(filename):
    with open(filename, 'rb') as file:
       return file.read()


'''
Write File as Bytes
'''
def write_file_in_bytes(filename,
content):
    with open(filename, 'wb') as file:
       file.write(content)


'''
Check Co Prime
Check if two numbers are coprime to each
other
'''
def check_co_prime(a, b):
      return math.gcd(a, b) == 1


'''
Generate RSA Key
Get a pair of public key and private key
'''
def generate_rsa_key(p, q, e=None):
      n, phi, k = p * q, (p - 1) * (q -
1), 1

      if not e:
      i = 2
      # Get the e starting from i = 2
      while not check_co_prime(i, phi):
            i += 1
      e = i

      # Calculate d
      d = (1 + (k * phi)) // e
      while ((1 + (k * phi)) / e) != d:
      k += 1
      d = (1 + (k * phi)) // e

      return ([e, n], [d, n])


'''
Hash Message
Hash message using SHA-3 and return the
hashed message
'''
def hash_message(encoded_string):
      hashed_message =
hashlib.new('sha3_512', encoded_string)
      return hashed_message.hexdigest()


'''
Sign Digital Signature
Sign digital signature using private key
'''
def sign_digital_signature(message, key):
      signature = int(message,
16)**key[0] % key[1]
      return '<ds>' + str(signature) +
'</ds>'
```

```
'''
Verify Signature
Verify Signature using public key
'''
def verify_signature(hashed_message,
signature, key):
      signature =
signature.replace(b'<ds>',
b'').replace(b'</ds>', b'')
      return int(signature)**key[0] %
key[1] == int(hashed_message, 16) %
key[1]


'''
Get Signature
Get signature of a content
'''
def scan_content(content, tag=b'<ds>'):
      try:
      i = content.index(tag)
      return (content[:i], content[i:])
      except Exception as e:
      return None


if __name__ == '__main__':
      pass
```

Kode program tersebut telah di-deploy di akun GitHub. https://github.com/darielgaizta/Cipherapp/blob/main/digital_signature/utils/digital_signature.py. Program tersebut berjalan dengan cara menerapkan fungsi hash pada isi konten struk belanja lalu memverifikasinya dengan kunci publik supermarket. Berikut merupakan gambar dari tampilan website supermarket yang bisa digunakan untuk memverifikasi struk belanja pembeli.

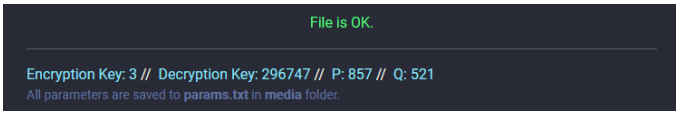


Gambar 4. Tampilan website supermarket untuk memverifikasi struk belanja.

Data struk belanja disimpan sebagai file teks dalam database supermarket dan kunci dekripsi disimpan dalam bentuk string. Isi dari file tersebut berupa barang-barang yang dibeli, tanggal pembelian, ID pembelian, total harga, dan tanda tangan digital. Berikut merupakan contoh isi dari file struk belanja.

```
Tanggal 22 Mei 2023
ID Pembelian: BDG87341098X1

Tempe 2000x4 = 8000
Jeruk 9000x1 = 9000

Total:  17000<ds>210307</ds>
```

Angka 210307 dalam tag <ds> merupakan tanda tangan digital untuk struk tersebut. Ketika seseorang ingin memverifikasi struk belanja, website akan melakukan pemindaian berdasarkan masukan berupa ID pembelian untuk mencari file terkait. Selanjutnya, website akan mulai memverifikasi struk belanja yang tersimpan di dalam database dengan menggunakan kunci dekripsi yang ada di database berdasarkan masukan ID pembelian. Jika struk belanja otentik, website akan memberitahu dengan pesan "File is OK" seperti pada Gambar 5. Untuk gambaran cara lebih lanjut, penjelasan terkait cara kerja pengimplementasian ini akan dijelaskan di bagian pengujian.



Gambar 5. Tanda bahwa struk belanja otentik.

B. Pengujian

Berikut merupakan contoh file struk belanja dari seorang pembeli.

```
Tanggal 22 Mei 2023
ID Pembelian: BDG87341098X1

Tempe 2000x4 = 8000
Jeruk 9000x1 = 9000

Total:  17000
```

Asumsikan bahwa supermarket memilih dua bilangan prima p dan q secara random dan didapat 857 dan 521. Dari kedua bilangan prima tersebut, didapatkan nilai hasil kali n, yaitu 446497. Kemudian, asumsikan lagi bahwa supermarket memilih angka 3 sebagai bilangan acak yang relatif prima terhadap $\phi(n)$ sehingga bisa didapatkan kunci d untuk

enkripsi pesan, yaitu 296747. Jadi, perhitungan untuk membangkitkan kunci RSA supermarket dapat dituliskan seperti berikut.

1. Dipilih dua bilangan prima acak p dan q, yaitu 857 dan 521
2. Hitung $\phi(n) = (p-1) \times (q-1)$, di mana $n = p \times q$. Dalam contoh ini, didapat nilai $\phi(n) = 445120$
3. Dipilih bilangan acak yang relatif prima terhadap $\phi(n)$. Dalam contoh ini, dipilih bilangan 3
4. Hitung nilai kunci untuk enkripsi d yang bisa dihitung dengan rumus $d = \frac{1+k\phi(n)}{e}$ sehingga didapat 296747

Selanjutnya, program akan langsung memberi tanda tangan pada struk belanja tersebut. Berikut merupakan bentuk final dari struk belanja yang didapat pembeli dan yang disimpan di dalam database supermarket.

```
Tanggal 22 Mei 2023
ID Pembelian: BDG87341098X1

Tempe 2000x4 = 8000
Jeruk 9000x1 = 9000

Total:  17000<ds>210307</ds>
```

Untuk proses verifikasi, pembeli atau petugas supermarket bisa pergi ke website resmi supermarket lalu memasukkan ID pembelian yang ada di struk. Berikut merupakan contoh tampilan website resmi supermarket.

Gambar 6. Tampilan website ketika ingin verifikasi struk.

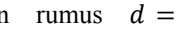
Jika struk masih asli, website akan menunjukkan pesan "Struk OK." seperti berikut.

Gambar 7. Tanda bahwa struk masih otentik.

Misal, isi dari struk diubah menjadi seperti berikut.

```
Tanggal 22 Mei 2023
ID Pembelian: BDG87341098X1

Tempe 2000x4 = 28000
Jeruk 9000x1 = 39000

Total:  67000<ds>280317</ds>
```

Jika struk sudah tidak lagi otentik atau sudah dimodifikasi, website akan menunjukkan pesan "Struk telah berubah." seperti berikut.



Gambar 8. Tanda bahwa struk telah berubah atau tidak otentik.

Perhatikan bahwa perubahan yang dilakukan pada struk terletak pada total harga dan tanda tangan digitalnya. Hal tersebut mungkin saja berhasil mengelabui petugas supermarket karena hasil hash (message-digest) bisa saja benar. Namun, website akan tetap mengeluarkan pesan "Struk telah berubah." karena website melakukan pengecekan dua kali, yaitu verifikasi tanda tangan dengan menggunakan kunci publik supermarket dan mencocokkan ID pembelian beserta tanda tangan digitalnya dengan yang ada dalam database.

IV. Kesimpulan

Implementasi tanda tangan digital dapat memberikan manfaat besar dalam meningkatkan efisiensi dan keamanan transaksi. Pnegimplementasian ini dapat mencegah ancaman-ancaman seperti adanya kasus penipuan pembeli yang menyalahkan struk karena telah memodifikasinya atau pegawai supermarket yang secara sengaja mengubah data record transaksi untuk seorang pembeli. Namun, ada tantangan yang perlu dihadapi dalam menjaga keamanan transaksi dengan menggunakan tanda tangan digital, seperti adanya pegawai yang berkhianat dan sengaja membocorkan keamanan data transaksi di supermarket. Meskipun begitu, penggunaan tanda tangan digital memberikan keuntungan yang cukup signifikan dalam hal menjaga keamanan karena dapat meningkatkan efisiensi penjagaan data transaksi dengan lebih efisien dan biaya yang lebih murah.

References

[1] Rinaldi Munir. 2023. Slide Kuliah II4031 Kriptografi dan Koding: Fungsi Hash.

[2] Rinaldi Munir. 2023. Slide Kuliah II4031 Kriptografi dan Koding: Algoritma RSA.

[3] Rinaldi Munir. 2023. Slide Kuliah II4031 Kriptografi dan Koding: Tanda Tangan Digital

[4] "Data Model–Python 3.10.4 Documentation" in *docs.python.org*. Retrieved 2023-05-22.

[5] "Digital Signatures and Certificates" in *support.microsoft.com*. Retrieved 2023-05-22.

[6] "What's a Digital Signature?" in adobe.com. Retrieved 2023-05-22.

[7] Paul, Eliza. 2017. "What is Digital Signature–How it works, Benefits, Objectives, and Concept". EMP Trust HR.

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