Sistem Pendataan Sensus Penduduk Berbasis *Digital Signature* Studi Kasus: Badan Pusat Statistik Kabupaten Aceh Utara

Nurmala Hayati[1], Salahuddin[2*], Musta'inul Abdi[3]

[1,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 Indonesia

[1]nurmala.hayati32@gmail.com

[2*]salahuddintik@pnl.ac.id

[3]mustainul.abdi@pnl.ac.id

Abstrak— **Sistem informasi memiliki peran penting dalam mendukung kegiatan operasional Badan Pusat Statistik (BPS), terutama dalam pengumpulan data untuk sensus dan survei. Unit kerja BPS, memiliki tantangan dalam mengumpulkan data yang representatif dan dapat dipertanggungjawabkan di wilayah yang luas dan padat penduduknya. Saat ini, BPS Kabupaten Aceh Utara masih menggunakan metode *Paper and Pencil Interview* (PAPI) yang kurang efektif dalam hal jumlah sampel yang cukup besar dan kontrol manajemen kualitas data. Untuk mengatasi permasalahan tersebut, BPS Kabupaten Aceh Utara membuat sistem yang dapat memvalidasi data pencacahan sensus penduduk dengan menggunakan *digital signature. Digital signature* atau tanda tangan digital adalah skema matematis yang digunakan untuk membuktikan keaslian pesan atau dokumen digital. Dalam pembuatan sistem pendataan tersebut digunakan algoritma DSA *(Digital Signature Algorithm).* DSA digunakan dalam aplikasi ini karena memenuhi DSS *(Digital Signature Standard),* yang telah diuji oleh NIST *(National Institute of Standards and Technology)* dan terbukti memiliki tingkat keamanan yang tinggi. Proses pembuatan tanda tangan digital diawali dengan pembuatan kunci publik dan kunci privat. Kunci publik akan digunakan untuk memverifikasi tanda tangan. Pada proses perhitungan nilai *hash* akan dihasilkan *message diggest,* yang akan digunakan dalam pembuatan tanda tangan. Proses penandatanganan menghasilkan sepasang tanda tangan (r,s). Pada proses verifikasi, akan mengecek apakah tanda tangan tersebut cocok atau tidak dengan menggunakan kunci publik dan menghitung nilai *hash* dokumen yang diterima. Adapun hasil akhir yang diperoleh adalah *digital signature*. Dari sebanyak 23 data yang sudah diuji dinyatakan sukses dan memperoleh hasil *digital signature.***

Kata kunci— Sensus, Penduduk, Digital Signature, Pendataan.

Abstract— ***Information systems have an important role in supporting the operational activities of the Central Bureau of Statistics (BPS), especially in collecting data for censuses and surveys. BPS work units have challenges in collecting representative and accountable data in a large and densely populated area. Currently, BPS Kabupaten Aceh Utara still uses the Paper and Pencil Interview (PAPI) method which is less effective in terms of a large enough sample size and data quality management control. To overcome these problems, BPS Kabupaten Aceh Utara created a system that can validate population census enumeration data using digital signature. Digital signature is a mathematical scheme used to prove the authenticity of a digital message or document. In making the data collection system, the DSA (Digital Signature Algorithm) algorithm is used. DSA is used in this application because it meets the DSS (Digital Signature Standard), which has been tested by NIST (National Institute of Standards and Technology) and proven to have a high level of security. The process of creating a digital signature begins with the creation of a public key and a private key. The public key will be used to verify the signature. In the hash value calculation process, a message diggest will be generated, which will be used in signature generation. The signing process produces a pair of signatures (r,s). In the verification process, it will check whether the signature matches or not by using the public key and calculating the hash value of the received document. The final result obtained is a digital signature. Of the 23 data that has been tested, it was declared successful and obtained a digital signature result.***

Keywords— Census, Population, Digital Signature, Data Collection.

I. PENDAHULUAN

Seiring berkembangnya teknologi di era modern, sistem informasi menjadi salah satu indikator penting dalam suatu instansi, terutama instansi pelayanan masyarakat yang memiliki tingkat rutinitas tinggi dan pengelolaan data yang terkelola.

Badan Pusat Statistik (BPS) adalah sebuah Lembaga Pemerintah Non-Kementerian yang bertanggung jawab langsung kepada Presiden dan bergerak di bidang penyediaan data statistik berkualitas melalui kegiatan statistik yang terintegrasi dan berstandar nasional maupun internasiona [1]. BPS berperan dalam menyelenggarakan sensus dan survei di seluruh wilayah Indonesia sesuai dengan kebutuhan data. Dalam mendukung kegiatan operasionalnya BPS tidak luput dari kebutuhan akan penggunaan sistem komputer terutama sistem informasinya.

Salah satu penggunaan sistem informasi di BPS adalah pada pelaksaan pengambilan data untuk sensus maupun survei untuk mendukung kegiatan pencacahan. Sistem informasi tersebut diharapkan dapat mendukung pencacah dalam pengambilan data yang sebenarnya.

BPS memiliki satuan kerja yang tersebar di seluruh wilayah Indonesia untuk membantu dalam memperoleh data dan informasi yang representatif dan dapat dipertanggungjawabkan. Salah satunya ialah Badan Pusat Statistik (BPS) Kabupaten Aceh Utara.

BPS Kabupaten Aceh Utara adalah unit kerja BPS yang memiliki wilayah tugas di kabupaten Aceh Utara. Dalam perannya untuk menyelenggarakan survei dan sensus, terdapat tahap pengumpulan data yang memerlukan sumber daya tenaga dari pihak luar dikarenakan keterbatasan pegawai di BPS Kabupaten Aceh Utara. Wilayah daerah Kabupaten Aceh Utara pada tahun 2022 mencapai 3.296,86 Km2 dengan 27 kecamatan dan 852 desa dan jumlah penduduknya kurang lebih 614,64 ribu [2].

Pada saat ini, BPS Kabupaten Aceh Utara masih menggunakan metode *Paper and Pencil Interview* (PAPI) dalam pelaksaan kegiatan survei maupun sensus, di mana metode ini masih memerlukan instrumen berupa kuesioner kertas. Dengan wilayah kabupaten Aceh Utara yang luas didukung dengan banyaknya kecamatan dan desa, pelaksanaan survei pada wilayah kabupaten Aceh Utara tentunya akan mengambil jumlah sampel yang cukup besar. Sehingga penggunaan kuesioner kertas ini dapat menjadi tidak praktis. Selain itu, kontrol manajemen kualitas data juga kurang praktis untuk dilakukan pada metode PAPI karena kurangnya media pengawasan, sehingga memungkinkan kesalahan atau kecurangan pada pengisian kuesioner di lapangan [3].

Dengan permasalahan yang telah diuraikan diatas maka dibuatlah suatu sistem yang dapat memvalidasi data pencacahan sensus penduduk. Validasi yang digunakan berupa *digital signature*. *Digital signature* atau tanda tangan digital adalah skema matematis yang digunakan untuk membuktikan keaslian pesan atau dokumen digital. Skema ini menjadi jaminan bahwa data dan informasi benar-benar berasal dari sumber yang benar, sehingga meminimalisir terjadinya kecurangan. Terdapat banyak algoritma kunci asimetris namun yang memenuhi DSS (*Digital Signature Standart*) hanya ada beberapa saja. Salah satunya adalah DSA (*Digital Signature Algorithm*) [4]. Algoritma ini telah diuji NIST (*National Institute of Standards and Technology*) dan terbukti memiliki tingkat kemanan yang tinggi. Algoritma DSA telah memenuhi kriteria yang dibutuhkan untuk mengatasi masalah yang ada [5].

Adapun tujuan untuk penelitian ini adalah merancang dan membangun sistem pendataan sensus berbasis digital signature serta menerapkan algoritma DSA dalam sistem pendataan sensus berbasis digital signature..

Manfaat dari penilitian ini adalah sistem pendataan sensus ini mempermudah mitra lapangan dalam mendata tanpa membawa dokumen kuesioner beserta alat tulis lainnya dan memperoleh sistem yang berfungsi untuk pendataan pada sensus yang dapat diakses menggunakan android, dengan menerapkan algoritma DSA.

II. METODOLOGI PENELITIAN

A. *Fungsi Hash Sha*

Fungsi *hash* adalah sebuah fungsi yang menerima masukan *string* yang panjangnya sembarang dan mengkonversikannya menjadi *string* keluaran yang panjangnya tetap (*fixed*) dan umumnya jauh lebih kecil dibandingkan *string* semula. Fungsi *hash* satu arah (*One way Hashing*) adalah fungsi *hash* yang bekerja dalam satu arah. Pesan yang sudah diubah menjadi *message digest* tidak dapat lagi dikembalikan menjadi pesan semula. Dua pesan yang berbeda akan selalu menghasilkan nilai *hash* yang berbeda pula. Sehingga *message digest* dari sebuah *string* dapat dijadikan sebagai sebuah sidikjari. Sifat-sifat fungsi *hash* kriptografi [6].

1. Preimage resistant

Bila diketahui nilai *hash h* maka sulit untukmendapatkan *m* dimana *h* = *hash*(*m*).

2. Second Preimage resistant

Jika diketahui input m_1 maka sulit mencari input m_2 (tidak sama dengan m_1) yang menyebabkan *hash* (m_1) = *hash* (m_2).

3. Collision-resistant

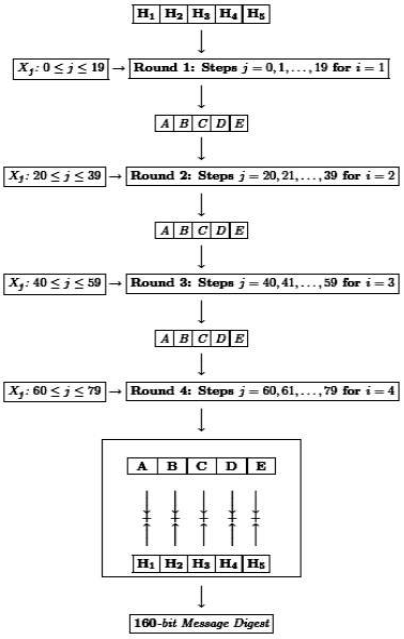
Sulit mencari dua input berbeda m_1 dan m_2 yang menyebabkan *hash* (m_1) = *hash*(m_2) yang termasuk dalam algoritma fungsi *hash* satu arah adalah MD5, MD6, SHA-1, SHA-224, SHA-256, SHA-384 dan lain-lain.

B. *Fungsi One-Way Hash SHA-1*

Secure Hash Algorithm (SHA-1) dikembangkan oleh NSA pada tahun 1995 dan distandarisasi oleh NIST (National Institute of Standard and Technology). SHA-1 merupakan algoritma *hash* searah dengan panjang maksimal untuk suatu *string* yang dapat di proses adalah 2^{64} *bit*. SHA-1 akan menghasilkan keluaran sebanyak 160 bit dari *string* tersebut. Berdasarkan cirinya SHA-1 dapat digunakan dengan algoritma kriptografi lainnya seperti *Digital Signature Algorithms* atau dalam generasi angka yang acak (*bits*). SHA-1 dikatakan aman

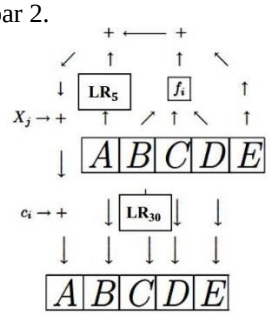
karena proses SHA-1 dihitung secara infisibel untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat juga digunakan untuk mencari dua *string* yang berbeda yang akan menghasilkan *message digest* yang sama. Proses pada algoritma ini antara lain:

1. Pesan diubah menjadi *bitstream*.
2. Hitung *g* = Panjang *bitstream* mod 512 jika.
   g < 448*bit* tambahkan sebuah *bit* 1 dan 447- *g bit* 0 pada data.
   g >= 448*bit* tambahkan sebuah *bit* 1 dan 959 - *g bit* 0 pada data.
3. Ubah panjang pesan dalam bentuk 64*bit* kemudian tambahkan pada akhir datayang akan di-*hash*.
4. Data yang akan di-*hash* dipecah-pecah menjadi bagian–bagian dengan panjangsebesar 512 *bit.*
5. Inisialisasi variabel, nilai variable c_1, c_2, c_3, c_4, h_0, h_1, h_2, h_3,
6. Setiap blok berukuran 512*bit* dipecah menjadi 16 bagian masing-masing berukuran 32-*bit* (*bitword*). Dari 16 *bitword* tersebut akan dihasilkan *bitword* ke 17 sampai *bitword* ke 80 dengan menggunakan algoritma *for i* 16 to 79 data(*i*) = LR_1(*i* - 3*XORi* - 8*XORi* -14 *XORi* -16).
7. Initialisasi varaibel *A, B, C, D, E*
   $A = h_0$, $B = h_1$, $C = h_2$, $D = h_3$, $E = h4$.
8. Untuk setiap *bitword* dilakukan perubahan variabel *A, B, C, D* ialah.
   a) Jika *bitword* ke-0 sampai *bitword* ke-19: $t = LR_5(A) + ((B\ AND\ C)\ OR\ (NOT(B)\ AND\ D)) + E + X_j + c_1$. Hapus *bit* paling kiri sampai *t* berukuran 32 *bit*. *E = D, D = C, C =* $LR_{30}(B)$, *B = A, A = t.*
   b) Jika *bitword* ke-20 sampai *bitword* ke-39:
   $t = LR_5(A) + (B\ XOR\ C\ XOR\ D) + E + X_j + c_2$.
   Hapus *bit* paling kiri sampai *t* berukuran 32 *bit*.
   E = D, D = C, C = $LR_{30}(B)$, *B = A, A = t.*
   c) Jika *bitword* ke-40 sampai *bitword* ke-59:
   t = LR5 (A) + (B AND C) OR (B AND D) OR (C AND D) + E + X j + c3. Hapus *bit* paling kiri sampai *t* berukuran 32 *bit*. *E = D, D = C, C =* $LR_{30}(B)$, *B = A, A = t.*
   d) Jika *bitord* ke-60 sampai *bitword* ke-79:
   $t = LR_5(A) + (B\ XOR\ C\ XOR\ D) + E + X_j + c_4$. Hapus *bit* paling kiri sampai *t* berukuran 32 *bit*. *E = D, D = C, C =* $LR_{30}(B)$, *B = A, A = t.*
9. Ubah variable h_0, h_1, h_2, h_3, h_4 dengan rumus
   $h_0 = h_0 + A$. Hapus *bit* paling kiri sampai h_0 berukuran 32 *bit*.
   $h_1 = h_1 + B$. Hapus *bit* paling kiri sampaih_1 berukuran 32 *bit*.
   $h_2 = h_2 + C$. Hapus *bit* paling kiri sampai h_2 berukuran 32 *bit*.
   $h_3 = h_3 + D$. Hapus *bit* paling kiri sampai h_3 berukuran 32 *bit*.
   $h_4 = h_4 + E$. Hapus *bit* paling kiri sampai h_4 berukuran 32 *bit*.
10. Lakukan pada blok 512*bit* lainnya.
11. Hasil dari proses di atas yaitu h_0, h_1, h_2, h_3, h_4 kemudian digabung. $h = LS_{128}(h_0)\ OR\ LS_{96}(h_1)\ OR\ LS_{64}(h_2)\ OR\ LS_{32}(h_3)\ OR\ h_4$.



Gambar 1. Proses SHA-1 untuk setiap 512bit blo*k*

Untuk proses SHA-1 hashing setiap bitwordnya dapat dilihat pada Gambar 2.



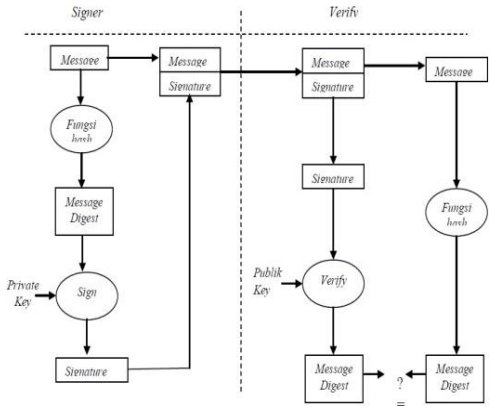
Gambar 2. Proses SHA-1 untuk setiap bitword

C. Digital Signature Algorithm

Tandatangan digital adalah suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Pada Agustus 1991, NIST(*The National of Standard and Technology*) mengumumkan standard untuk tandatangan *digital* yang dinamakan *Digital Signature Standard* (DSS) yang terdiri dari dua komponen [7] :

1. Algoritma tandatangan digital disebut juga DSA (*Digital Signature Algorithm)*

2. Fungsi Hash disebut juga SHA (*Secure HashAlgorithm*). Jadi DSA untuk penandatanganan pesan dan SHA untuk membangkitkan *message digest* dari pesan.



Gambar 3. Diagram Proses Tanda Tangan Digital

1. Menentukan Parameter DSA
   a) p adalah bilangan prima dengan panjang L bit, dimana $2^{L-1} < p < 2^L$ dengan $512 \leq L \leq 1024$ dan L adalah kelipatan 64. Parameter p bersifat publik dan dapat digunakan bersama- sama oleh orang di dalam kelompok.
   b) q adalah bilangan prima 160 bit, faktor dari p- 1 dengan kata lain (p-1) mod q = 0. Parameter q bersifat publik dan dapat digunakan bersama-sama oleh orang di dalam kelompok dimana $2^{159} < q < 2^{160}$.
   c) Pembangkit g pada grup siklik tunggal dengan order q di dalam $Z_p{}^*$. Hitung g =h $^{(p-1)/q}$mod p, dengan h ∈ $Z_p{}^*$, 1< h < p – 1 sehingga g > 1. Parameter g bersifat publik dan dapat digunakan bersama-sama oleh orangdi dalam kelompok.
   d) x bilangan bulat dimana 0 < x < q denganpanjang 160 bit. Parameter x bersifat privat yang hanya boleh diketahui oleh pengirim pesan.
   e) $y = g^x \bmod p$ adalah kunci publik.
   f) M adalah pesan yang akan diberi tandatangan.
   g) k adalah bilangan bulat yang dibangkitkan random atau pseudorandom dimana 0<k< q. Parameter k bersifat privat yang hanya boleh diketahui oleh pengirim pesan.

Parameter p, q dan g bersifat publik dan dapat digunakan bersama dalam sekelompok orang. Parameter p, q dan g juga bernilai tetap untuk periode/waktu tertentu. Parameter x dan k hanyadigunakan untuk pembangkitan tandatangan dan harus dijaga kerahasiaannya. Parameter k harus berbeda untuk setiap tandatangan.

2. Pembentukan Sepasang Kunci

Input : Bilangan prima p dan q, dimana (p-1) mod q = 0, elemen primitif g, dimana g > 1 danbilangan x < q. Output : Kunci publik (p,q,g,y) dan kunci privat (p,q,g,x). Langkah untuk pembentuntukan sepasang kunci ialah.

1) Pilih bilangan prima p dan q, dimana (p-1)mod q = 0.
2) Hitung $g = h^{(p-1)/q} \bmod p$, dimana 1 < h < p–1dan g > 1.
3) Tentukan kunci privat x < q.
4) Hitung kunci publik $y = g^x \bmod p$.
5) Publikasikan p,q,g, dan y, tetapi nilai xdirahasiakan.

Kunci publik yang dihasilkan pada pembentukan kunci ini bersifat tunggal, karena ketiga nilai yang akan digunakan pada pembentukan kunci sudah ditetapkan, sehingga nilaiy adalah tunggal.

Terdapat y_1 dan y_2. Diambil bilangan prima p danq, dimana (p – 1) mod q = 0,

$g = h^{(p-1)/q} \bmod p$, dimana 1 < h < p-1 dan g > 1 danx < q.Dengan $y = g^x \bmod p$, maka

$$y_1 = g^x \bmod p \quad (1)$$

$$y_2 = g^x \bmod p \quad (2)$$

$y_1 = g^x \bmod p$, maka $g^x = y_1 \bmod p$ (3) (3) disubstitusikan ke dalam persamaan (2),sehingga

$y_2 = (y_1 \bmod p) \bmod p$

$y_2 = y_1 \bmod p$ (berdasarkan aturan aritmatikamodular)

Dengan demikian $y_2 = y_1$, terbukti bahwa kunci y bersifat tunggal.

3. Proses Penandatanganan

Input : Pesan M yang akan dikirimkan, dankunci privat x. Output : Pesan M dan tanda tangan (r,s) Langkah-langkah proses penandatanganan ialah.

1) Ubah pesan M menjadi *nilai hash* dengan fungsi Hash SHA-1menghasilkan SHA- 1(M).
2) Tentukan bilangan acak k < q.
3) Tanda tangan dari pesan m adalah bilangan r dan s yang didapat dari : r = (g^k mod p)mod q, s = (k^{-1} (SHA-1(M) + xr)) mod q. k^{-1} adalah invers dari k modulo q, dengan $k.k^{-1} \equiv 1 \bmod q$. Pada perhitungan nilai s, 160-bit barisan hingga SHA-1(M) dikonversi terlebih dahulu ke dalam bilangan bulat. Jikatandatangan yang dihasilkan benar makanilai r dan atau s tidak mungkin 0.
4) Kirim pesan beserta tandatangan r dan s.

4. Proses Verifikasi

Setelah pesan telah sampai kepada pihak penerima, maka penerima akan melakukanproses verifikasi. Untuk melakukan proses ini, penerima pesan menggunakan kunci publik (p,q,g,y) yang telah diberikan dari pengirim pesan. Penerima memperoleh pesan yang berupa dokumen yang telah dibubuhi tanda tangan digital. Dalam hal ini, dokumen bisasaja berupa *plaintext* maupun *ciphertext.* Tergantung dari perjanjian antar pihak yang bersangkutan. Sebelumnya akan dihitung terlebih dahulu nilai *hash* dari dokumen yang diterima. Kemudian penerima akan memverifikasi tanda tangan (r, s). terlebih dahulu ia akan mengecek 0 < r < q and 0 < s < q kemudian menghitung:

$w = s^{-1} \bmod q$

$u_1 = (\text{SHA-1(M)} * w) \bmod q$ $u_2 = (r * w) \bmod q$

$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q)$

Jika v = r maka tandatangan sah, pesan yang diterima dikirim oleh pihak memegangkunci rahasia x sesuai dengan y kunci publiknya, dengan kata lain pesan masih asli dan dokumen dikirim oleh pengirim yangbenar.

Jika v != r, maka terdapat beberapakemungkinan yaitu pesan telah dimodifikasi, pesan telah salah ditandatangani oleh

penandatangan, ataupesan telah ditandatangani oleh pihak lain (bukan penandatangan sebenarnya) berarti pesan tidak valid.

D. Sensus

Sensus adalah metode untuk mengumpulkan informasi melalui pengumpulan data dari seluruh populasi. Tujuannya adalah untuk memperoleh gambaran yang akurat dan detail tentang populasi yang diteliti, termasuk informasi demografis, pendidikan, pekerjaan, dan pendapatan. Sensus dilakukan setiap beberapa tahun dan melibatkan pengumpulan data dari setiap individu dalam populasi . Dalam peraturan pemerintah sensus [8].

1. Sensus penduduk

Sensus penduduk adalah cara pengumpulan data yang dilakukan melalui pencacahan seluruh penduduk yang bertempat tinggal atau berada di wilayah Republik Indonesia untuk memperoleh karakteristik penduduk pada saat tertentu.

2. Sensus pertanian

Sensus pertanian adalah cara pengumpulan data yang dilakukan melalui pencacahan seluruh petani, rumah tangga pertanian, dan perusahaan pertanian di wilayah Republik Indonesia untuk memperoleh karakteristik pertanian pada saat tertentu.

3. Sensus ekonomi

Sensus ekonomi adalah cara pengumpulan data yang dilakukan melalui pencacahan seluruh usaha dan atau perusahaan non pertanian di wilayah Republik Indonesia untuk memperoleh karakteristik usaha dan atau perusahaan pada saat tertentu . Waktu penyelenggaraan sensus, dilaksanakan pada:

a) tahun berakhiran angka 0 (nol) bagi sensus penduduk.
b) tahun berakhiran angka 3 (tiga) bagi sensus pertanian.
c) tahun berakhiran angka 6 (enam) bagi sensus ekonomi.

E. Survei

Survei adalah cara pengumpulan data yang dilakukan melalui pencacahan sampel dari sesuatu populasi untuk memperkirakan karakteristik suatu obyek pada saat tertentu. Tujuannya adalah untuk memperoleh gambaran umum tentang subjek yang diteliti. Survei dapat dilakukan melalui berbagai metode, seperti wawancara, kuesioner, atau observasi.

F. UML(Unified Modeling Language)

UML (Unified Modeling Language) adalah sebuah bahasa visual yang digunakan dalam pengembangan software untuk memodelkan dan menggambarkan struktur dan perilaku sistem yang akan dibangun. UML digunakan oleh pengembang software untuk memahami, merancang, dan mengembangkan sistem yang kompleks dengan cara yang terstruktur dan terdokumentasi dengan baik. UML terdiri dari beberapa jenis diagram yang masing-masing memiliki kegunaan dan tujuan berbeda, berikut jenis diagramnya.

1. Use Case Diagram : Digunakan untuk menggambarkan interaksi antara actor dengan sistem yang dibangun.
2. Class Diagram : Digunakan untuk menggambarkan struktur sistem yang dibangun, terutama pada tingkat class.
3. Sequence Diagram : Digunakan untuk menggambarkan urutan interaksi antara objek dalam sebuah proses atau kasus penggunaan.
4. Activity Diagram : Digunakan untuk menggambarkan alur atau urutan aktivitas yang terjadi dalam sebuah proses.
5. State Machine Diagram : Digunakan untuk menggambarkan perilaku dari objek atau sistem dalam berbagai keadaan atau kondisi.
6. Component Diagram : Digunakan untuk menggambarkan struktur komponen sistem dan hubungan antara komponen-komponen tersebut.
7. Deployment Diagram:Digunakan untuk menggambarkan bagaimana sistem akan di-deploy atau diimplementasikan pada lingkungan fisik atau jaringan.

G. Pengujian System

1. Pengujian *Black Box*

Black box Testing atau pengujian kotak hitam merupakan teknik pengujian software yang berfokus pada spesifikasi fungsional dari *software*. Pengujian *black box* bekerja tanpa memperhatikan struktur internal dari kode program atau sistem yang diuji, pengujian dilakukan dari sudut pandang pengguna atau aktor yang berinteraksi dengan sistem.

2. Pengujian *White Box*

Pengujian *white box* dilakukan untuk pengujian algoritma DSA pada sistem. Penggunaan *white box* akan menguji masing masing fungsi, komponen maupun proses dalam mendapatkan *output.*

3. Pengujian Kepuasan Pengguna

Pengujian kepuasan pengguna dilakukan menggunakan kuesioner data untuk mendapatkan data berupa tingkat kepuasan atas aplikasi sistem pendataan sensus penduduk, baik dari segi UI/UX serta kinerja aplikasi.

III. HASIL DAN PEMBAHASAN

A. Hasil Pengujian Black-box

1. Pengujian Halaman Login

TABEL I
PENGUJIAN HALAMAN LOGIN

No	Fungsi yang diuji	Hasil yang diharapkan	Respond Sistem	Kesimpulan
1	Masukkan email	Muncul halaman utama	Tampil masukan email	Berhasil
2	Masukkan password	Muncul halaman utama	Tampil masukan password	Berhasil
3	Masuk	Muncul halaman utama	Masuk ke halaman dashboard	Berhasil

Masukan yang diuji pada halaman login ialah masukkan email dan password. Pengujian akhir dilakukan pada tombol masuk untuk menuju halaman utama apabila telah selesai melakukan login. Sistem berhasil merespon semua pengujian yang dilakukan sehingga dapat disimpulkan pengujian halaman login berhasil.

2. Pengujian Halaman Registrasi

TABEL II
PENGUJIAN HALAMAN REGISTRASI

No	Fungsi yang diuji	Membuat akun baru	Respond Sistem	Kesimpulan
1	Masukkan nama	Membuat akun baru	Tampil masukkan nama	Berhasil
2	Masukkan email	Membuat akun baru	Tampil masukkan email	Berhasil
3	Masukkan kata sandi	Membuat akun baru	Tampil masukkan kata sandi	Berhasil
4	masukkan konfirmasi kata sandi	Membuat akun baru	Tampil masukkan konfirmasi kata sandi	Berhasil
5	Daftar	Membuat akun baru	Masuk ke halaman utama	Berhasil

Masukan yang diuji pada halaman registrasi ialah masukkan nama, email password dan konfirmasi password. Pengujian akhir dilakukan pada tombol daftar untuk menuju halaman utama apabila telah selesai melakukan registrasi. Sistem berhasil merespon semua pengujian yang dilakukan sehingga dapat disimpulkan pengujian halaman registrasi berhasil.

3. Pengujian Halaman Utama

TABEL III
PENGUJIAN HALAMAN UTAMA

No	Fungsi yang diuji	Hasil yang diharapkan	Respond Sistem	Kesimpulan
1	Tombol halaman utama	Menampilkan halaman utama	Tampil halaman utama	Berhasil
2	Tombol halaman kuesioner mitra	Menampilkan halaman kuesioner mitra	Tampil halaman kuesioner mitra	Berhasil
3	Tombol halaman akun anda	Menuju halaman akun anda	Masuk halaman akun anda	Berhasil

Pengujian halaman utama bertujuan untuk fungsi tombol pada halaman utama. Tombol-tombol yang ada di tabel mitra ialah halaman utama, halaman kuesioner dan halaman akun.

4. Pengujian Halaman Akun

TABEL IV
PENGUJIAN HALAMAN AKUN

No	Fungsi yang diuji	Hasil yang diharapkan	Respond Sistem	Kesimpulan
1	perbaharui nama	Menampilkan nama baru	Tampil nama	Berhasil
2	perbaharui email	Menampilkan email baru	Tampil email	Berhasil
3	upload foto	Menampilkan poto	Tampil poto	Berhasil
4	hapus foto	menghapus poto	hapus poto	Berhasil
5	Keluar	Menampilkan halaman login	Masuk ke halaman login	Berhasil

Tampilan yang diuji pada halaman akun anda ialah menampilkan nama, email, NIK, upload poto, hapus poto dan *logout*. Pengujian akhir dilakukan pada tombol keluar untuk menuju halaman *login* apabila telah selesai melihat akun anda. Sistem berhasil merespon semua pengujian yang dilakukan sehingga dapat disimpulkan pengujian halaman akun anda berhasil.

5. Pengujian Halaman Mitra

TABEL V
PENGUJIAN HALAMAN MITRA

No	Fungsi yang diuji	Hasil yang diharapkan	Respond Sistem	Kesimpulan
1	memblokir akun	Menampilkan nama akun yang diblokir	Tampil nama pada diblokir	Berhasil
2	membatalkan blokir	Menampilkan nama akun pada list aktif	Tampil nama pada aktif	Berhasil

Tampilan yang diuji pada halaman mitra ialah menampilkan nama akun mitra yang berhasil login dan nama mitra yang di blokir oleh admin.

6. Pengujian Halaman Korsel

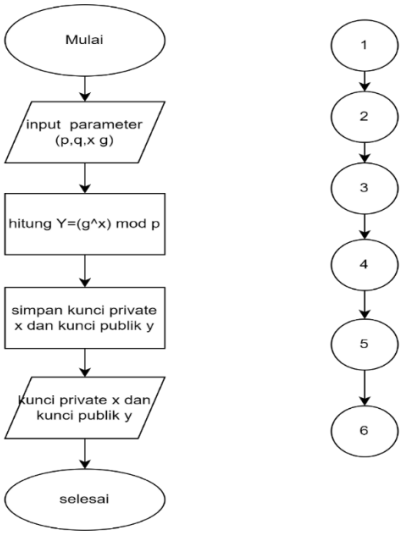
TABEL VI
PENGUJIAN HALAMAN KORSEL

No	Fungsi yang diuji	Hasil yang diharapkan	Respond Sistem	Kesimpulan
1	tambah gambar	menampilkan gambar korsel	Tampil gambar korsel	Berhasil
2	perbaharui gambar	Menampilkan gambar korsel yang baru	Tampil gambar korsel	Berhasil
3	hapus gambar	menghapus gambar korsel	hapus gambar korsel	Berhasil

Pengujian halaman korsel bertujuan untuk fungsi tombol pada halaman utama. Tombol-tombol yang ada di halaman korsel ialah tambah gambar, perbaharui gambar dan hapus gambar.

B. Hasil Pengujian White-box

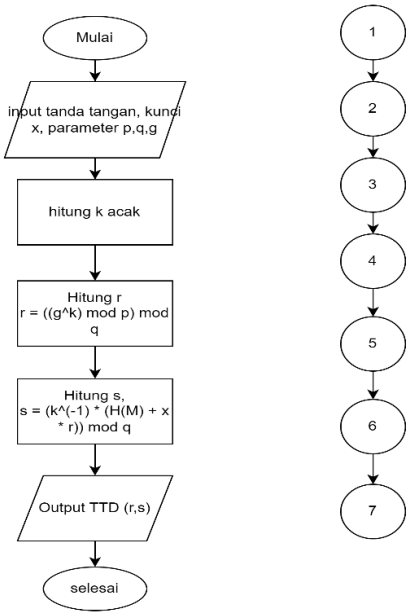
Pengujian *white-box* merupakan tipe pengujian perangkat lunak di mana penguji memiliki pengetahuan dan akses lengkap terhadap struktur internal, kode sumber, dan logika dari aplikasi yang sedang diuji. Tujuan dari pengujian *white-box* adalah untuk mengidentifikasi potensi kelemahan dalam kode sumber, urutan eksekusi, dan logika aplikasi yang mungkin tidak terdeteksi oleh pengujian *black-box*. Hal ini berbeda dengan pengujian *black-box* di mana penguji hanya fokus pada input dan output tanpa mengetahui secara detail cara kerja sistem di dalamnya. Dalam pengujian *white-box*, penguji memiliki pandangan yang lebih mendalam tentang komponen-komponen internal aplikasi tersebut. Pengujian *white-box* dapat dilihat pada Gambar 4.



Gambar 4. Flowchart dan flowgraph whitebox pembangkit kunci.

Jalur 1: 1-2-3-4-5-6
Case Pembangkitan Kunci :
Path: 1
Jalur: 1-2-3-4-5-6
Skenario :
1. Start
2. Input p,q,dan g
3. Menghitung y=(g^x) mod p
4. Menyimpan kunci public x dan kunci private y
5. Hasilnya kunci public dan kunci private
6. Selesai

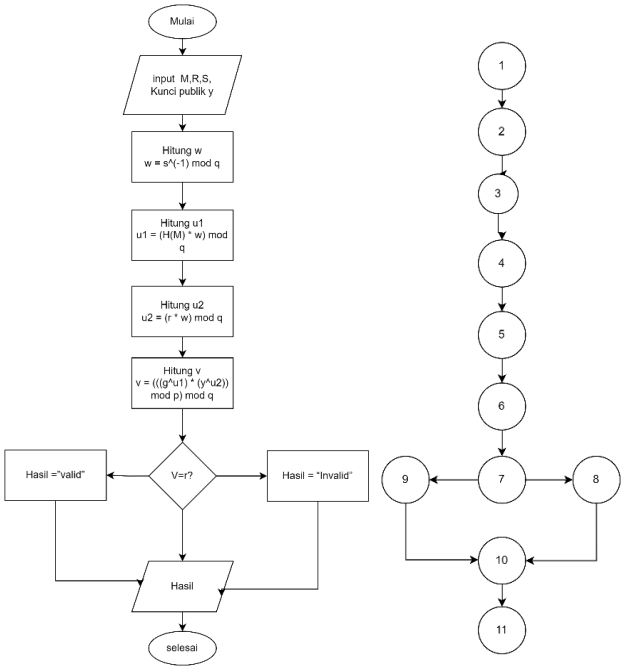
Hasil pengujian: Berhasil



Gambar 5. Flowchart dan flowgraph tanda tangan

Jalur : 1-2-3-4-5-6
Case Tanda Tangan:
Path: 1
Skenario :
1. Start
2. input tanda tangan, kunci x, parameter p,q,g
3. hitung k acak
4. Hitung r = ((g^k) mod p) mod q
5. Hitung s, s = (k^(-1) * (H(M) + x * r)) mod q
6. Output TTD (r,s)
7. Selesai

Hasil pengujian: Berhasil



Gambar 6. Flowchart dan flowgraph verifikasi

Jalur 1: 1-2-3-4-5-6-7-8-10-11
Jalur 2: 1-2-3-4-5-6-7-9-10-11
Case Verifikasi:
Path: 1
Jalur: 1-2-3-4-5-6-7-8-10-11
Skenario :
1. Start
2. input M,R,S, Kunci publik y
3. Hitung w, w = s^(-1) mod q
4. Hitung u1, u1 = (H(M) * w) mod q
5. Hitung u2, u2 = (r * w) mod q
6. Hitung v, v = (((g^u1) * (y^u2)) mod p) mod q
7. V=r?
8. Hasil = “Invalid”
9. Hasil
10. Selesai

Hasil pengujian: Berhasil

Path: 2
Jalur: 1-2-3-4-5-6-7-9-10-11
Skenario :
1. Start
2. input M,R,S, Kunci publik y
3. Hitung w, w = s^(-1) mod q
4. Hitung u1, u1 = (H(M) * w) mod q
5. Hitung u2, u2 = (r * w) mod q
6. Hitung v, v = (((g^u1) * (y^u2)) mod p) mod q
7. V=r?
8. Hasil = "valid"
9. Hasil
10. Selesai

Hasil pengujian: Berhasil

Dari hasil pengujian yang telah dilakukan, dapat diketahui bahwa pengujian pada algoritma DSA berhasil melalui beberapa alur, sehingga algoritma tersebut dapat disimpulkan menyesuaikan arah atau alur sesuai dengan proses yang dilakukan. Adapun hasil keseluruhan dari pengujian algoritma DSA adalah berhasil.

C. Hasil Pengujian Kuesioner

Pengujian kuesioner ini dilakukan dengan tujuan untuk memahami tingkat kepuasan pengguna dalam menggunakan sistem pendataan sensus. Hasil pengujian diperoleh melalui penyebaran kuesioner kepada 25 responden, yang masing masing menjawab 10 pertanyaan. Berikut data yang terkumpul dapat dilihat pada table 7.

TABEL VII
HASIL KUESIONER

Pertanyaan	Sangat tidak puas	Tidak Puas	Netral	Puas	Sangat Puas
1	0	0	0	12	13
2	0	0	0	12	13
3	0	0	3	8	14
4	0	0	0	8	14
5	0	0	1	11	16
6	0	0	1	11	13
7	0	0	0	10	15
8	0	0	1	10	14
9	0	0	0	10	15
10	0	0	0	10	15
TOTAL	0	0	6	102	142

Berdasarkan hasil kuesioner di atas, selanjutnya dilakukan perhitungan untuk mendapatkan rata-rata dari jawaban pertanyaan kuesioner sebagai berikut.

$$\text{Rata-rata} = \frac{(0x19{,}99\%)+(0x39{,}99\%)+(6x59{,}99\%)+(102x79{,}99\%)+(142x100\%)}{(0+0+6+102+142)} \boldsymbol{X100\%}$$
$$= \frac{227{,}1892}{250} X100\%$$
$$= 90{,}88\%$$

Berdasarkan perhitungan di atas diketahui bahwa rata-rata nilai jawaban yang dihasilkan dari seluruh responden adalah sebesar 90.88% dengan keterangan (Sangat Puas). Sehingga dapat disimpulkan sistem yang dibangun dapat meningkatkan kepuasan pelanggan.

IV. SIMPULAN

Setelah melakukan perancangan dan pengujian pada sistem pendataan sensus penduduk berbasis *digital signature* pada BPS Kabupaten Aceh Utara dapat disimpulkan hasil analisa metode SHA dan DSA yang diterapkan kedalam sistem aplikasi digital signature dapat mempermudah proses pendataan sensus penduduk, algoritma SHA-1 dan DSA dapat melakukan proses pembuatantanda tangan digital dirahasiakan dalam bentuk kode acak dan aplikasi yang dibangun dapat membuktikan bahwa algoritma DSA dapat berjalan dengan baik, yang dibuktikan oleh hasil dari sebanyak 23 data yang sudah diuji dinyatakan sukses dan memperoleh hasil digital signature sesuai dengan yang diharapkan..

REFERENSI

[1] bps.go.id, "Informasi Umum BPS," *bps.go.id*, Feb. 20, 2023. https://ppid.bps.go.id/app/konten/0000/Profil-BPS.html (accessed Feb. 20, 2023).
[2] S. Direktorat, A. K. Statistik, P. Statistik, and B. P. Statistik, "Statistik Indonesia 2004 Statistical Year Book Of Indonesia 2004."
[3] P. Studi Manajemen and S. la Tansa Mashiro, "The Asia Pacific Journal of Management Studies Implementasi Rekrutmen Di Bps Kabupaten Lebak (Studi Kasus Rekrutmen Tenaga Sensus) Implementation, Census Partner Recruitment at BPS Lebak Regency".
[4] E. Andi Kriswanto, P. Studi Teknik Informatika, S. Banjarbaru, J. A. Yani Km, and K. Selatan, "Implementasi Digital Signature Untuk Validasi Disposisi Surat".
[5] F. Nurhasanah and R. Sulaiman, "Pembuatan Tanda Tangan Digital Menggunakan Digital Signature Algorithm."
[6] Yohanes, "Teknik Autentikasi." http://myeducationit.blogspot.com/2015/11/teknik-autentukasi.html
[7] M. Nurudin, W. Jayanti, R. D. Saputro, M. P. Saputra, and Y. Yulianti, "Pengujian Black Box pada Aplikasi Penjualan Berbasis Web Menggunakan Teknik Boundary Value Analysis," *Jurnal Informatika Universitas Pamulang*, vol. 4, no. 4, p. 143, 2019, doi: 10.32493/informatika.v4i4.3841.
[8] M. Ir. Yusuf Kurniawan, Kriptografi Keamanan Internet dan Jaringan Telekomunikasi.
[9] Z. A. Fikriya, M. I. Irawan, and S. Soetrisno., "Implementasi Extreme Learning Machine untuk Pengenalan Objek Citra Digital," J. Sains dan Seni ITS, vol. 6, no. 1, p. 18, 2017, doi: 10.12962/j23373520.v6i1.21754.
[10] T. Khotimah and R. Nindyasari, "Forecasting Dengan Metode Regresi Linier Pada Sistem Penunjang Keputusan Untuk Memprediksi Jumlah Penjualan Batik (Studi Kasus Kub Sarwo Endah Batik Tulis Lasem)," J. Mantik Penusa, vol. 1, no. 1, pp. 71–92, 2017.
[11] S. A. Alasadi and W. S. Bhaya, "Review of data preprocessing techniques in data mining," J. Eng. Appl. Sci., vol. 12, no. 16, 2017, doi: 10.3923/jeasci.2017.4102.4107.
[12] J. Adhiva, S. A. Putri, and S. G. Setyorini, "Prediksi Hasil Produksi Kelapa Sawit Menggunakan Model Regresi Pada PT . Perkebunan Nusantara V," pp. 155–162, 2020.
[13] I. Nabillah and I. Ranggadara, "Mean Absolute Percentage Error untuk Evaluasi Hasil Prediksi Komoditas Laut," vol. 5, no. 2, pp. 250–255, 2020, doi: 10.33633/joins.v5i2.3900.
[14] Verawati and P. D. Liksha, "Aplikasi Akuntansi Pengolahan Data Jasa Service," J. Sist. Inf. Akunt., vol. 1, no. 1, p. 3, 2018.