Tanda-tangan Digital

Review materi awal

- Ingat kembali empat layanan keamanan yang disediakan oleh kriptografi:
  1. Kerahasiaan pesan (*confidentiality/secrecy*)
  2. Keaslian pesan (*data integrity*).
  3. Otentikasi (*authentication*)
  4. Anti-penyangkalan (*nonrepudiation*).

- Layanan 1 dilakukan dengan mengenkripsi/dekripsi pesan
- Layanan 2 dilakukan dengan fungsi hash dan MAC
- Layanan 3 dilakukan dengan menggunakan MAC dan tanda-tangan digital (*digital signature*).
- Layanan 4 dilakukan dengan menggunakan tanda-tangan digital (*digital signature*).

Tanda-tangan

- Sejak zaman dahulu, tanda-tangan sudah digunakan untuk otentikasi dokumen cetak.

- Tanda-tangan mempunyai karakteristik sebagai berikut:
  1. Tanda-tangan adalah bukti yang otentik.
  2. Tanda tangan tidak dapat dilupakan.
  3. Tanda-tangan tidak dapat dipindah untuk digunakan ulang.
  4. Dokumen yang telah ditandatangani tidak dapat diubah.
  5. Tanda-tangan tidak dapat disangkal.

Hari: Senin, Tanggal 12 September 2016

Waktu: 14.00 Wib

Tempat: Aula

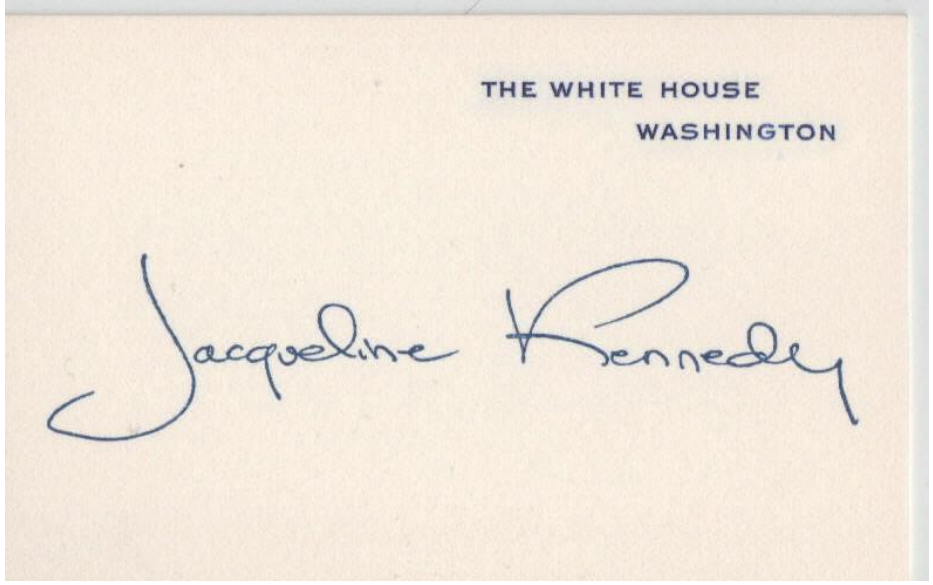
Demikian kami buat surat ini dengan sebenarnya. Harap semua peserta untuk hadir sesuai jadwal yang telah disebutkan di atas. Terima kasih.

Tertanda tangan

Mr Mukidi

Master of Ceremony
Doktor Mukidi, Mpd

- Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data digital (pesan, dokumen elektronik).
- Tanda-tangan untuk data digital dinamakan **tanda-tangan digital** (*digital signature*).
- Tanda-tangan digital di dalam konteks kriptografi tidak sama dengan tanda-tangan yang di-digitisasi (*digitized signature*) dengan cara dipindai atau difoto.



digitized signature

digitized signature

- Tanda-tangan digital adalah *nilai kriptografis* yang bergantung pada isi pesan dan kunci.

- Jika tanda-tangan seseorang pada dokumen cetak selalu sama, apa pun isi dokumennya,

- maka tanda-tangan digital selalu berbeda-beda antara satu pesan dengan pesan lain, dan/atau antara satu kunci dengan kunci yang lain.

Paris, 31 Desember 2018

Halo Alice
Sudah lama kita tidak berjumpa sejak lulus SMA. Saya sekarang tinggal di Paris sejak tahun 2016. Saya bekerja di sebuah perusahaan IT yang bernama Solution Express. Perusahaan ini memberikan layanan keamanan informasi berbasis cloud computing. Saya menjadi menejer Quality Control. Klien kami umumnya adalah bank-bank yang membutuhkan keamanan data nasabah.

Oh ya, saya belum menanyakan bagaimana keadaanmu sekarang. Di mana kamu bekerja atau malah melanjutkan studi S2 di mana? Saya ingat kamu dulu jago sekali pelajaran kimia. Apakah kamu masih menekuni bidang kimia saat ini?

Oke deh, jika kamu jalan-jalan ke Eropa jangan lupa mampir ke kota Paris. Nanti saya akan ajak kamu mengunjungi Menara Eiffel. Bisa naik sampai ke atas lho.

Salam dari temanmu di Paris
Bob

-- BEGIN SIGNATURE --
13706B6D42442620B2FD1098BD4D54ADFA9F7DC27576954ADCE5E5FC901
-- END SIGNATURE--

Persyaratan Tanda Tangan Digital

1. Tanda tangan harus berupa rangkaian bit yang bergantung pada pesan yang ditandatangani
2. Tanda tangan harus menggunakan informasi yang unik (=kunci) dari pengirim untuk mencegah pemalsuan dan penyangkalan
3. Membangkitkan tanda tangan digital harus relatif mudah dilakukan
4. Mengenali dan memverifikasi tanda tangan digital harus relatif mudah dilakukan
5. Secara komputasi hampir tidak mungkin memalsukan tanda tangan digital, baik dengan merekonstruksi pesan baru untuk tanda tangan digital yang sudah ada, atau merekonstruksi tanda tangan curang untuk pesan yang diberikan
6. Menyimpan salinan tanda tangan digital ke dalam storage harus mudah dilakukan secara praktek.

Dua proses dalam tanda-tangan digital

1. Menandatangani pesan (*signing*)
   Memberi tanda-tangan pada pesan

2. Memverifikasi tanda-tangan (*verification*)
   Memeriksa keabsahan tanda-tangan digital

Tanda-tangan Digital Menggunakan Kombinasi Kriptografi kunci-publik dan Fungsi *Hash*

- Kombinasi algoritma kriptografi kunci-publik dan fungsi *hash* dapat digunakan untuk tanda-tangan pesan digital.

- Mula-mula pesan (M) dihitung nilai *hash*-nya dengan fungsi hash (misalnya MD5 atau SHA-1). Hasilnya adalah *message digest* (h).

- Selanjutnya *message digest* dienkripsi dengan **kunci privat** si pengirim pesan (*signer*). Hasil enkripsinya dinamakan tanda-tangan digital (S).

- Pesan M dan tanda-tangan S dikirim ke penerima pesan

- Di sisi penerima pesan (*vervyer*), ia memisahkan tanda-tangan digital dengan pesan

  (a) Pesan M dihitung *nilai-hash* nya dengan fungsi *hash* yang sama, hasilnya message digest (h).

  (b) Tanda-tangan digital S didekripsi dengan **kunci publik** si pengirim pesan, hasilnya *message digest* (h)

  (c) Jika *message digest* dari proses (a) sama dengan *message digest* dari proses (b), maka tanda-tangan digital sah (valid) atau terverifikasi.

- Jika tanda-tangan digital valid, maka itu artinya:

  (a) Pesan berasal dari pengirim yang sesungguhnya (pengirim pesan terotentikasi)

  (b) Pesan masih asli/utuh, tidak mengalami perubahan (integritas pesan benar)

  (c) Pengirim pesan tidak dapat menyangkal telah mengirim pesan

Alice

Signer

Verifier

Bob

Message

Fungsi
Hash

Message
Digest (MD)

Private
Key Alice

Encrypt

Signature

Message

Signature

Message

Signature

Public
Key Alice

Decrypt

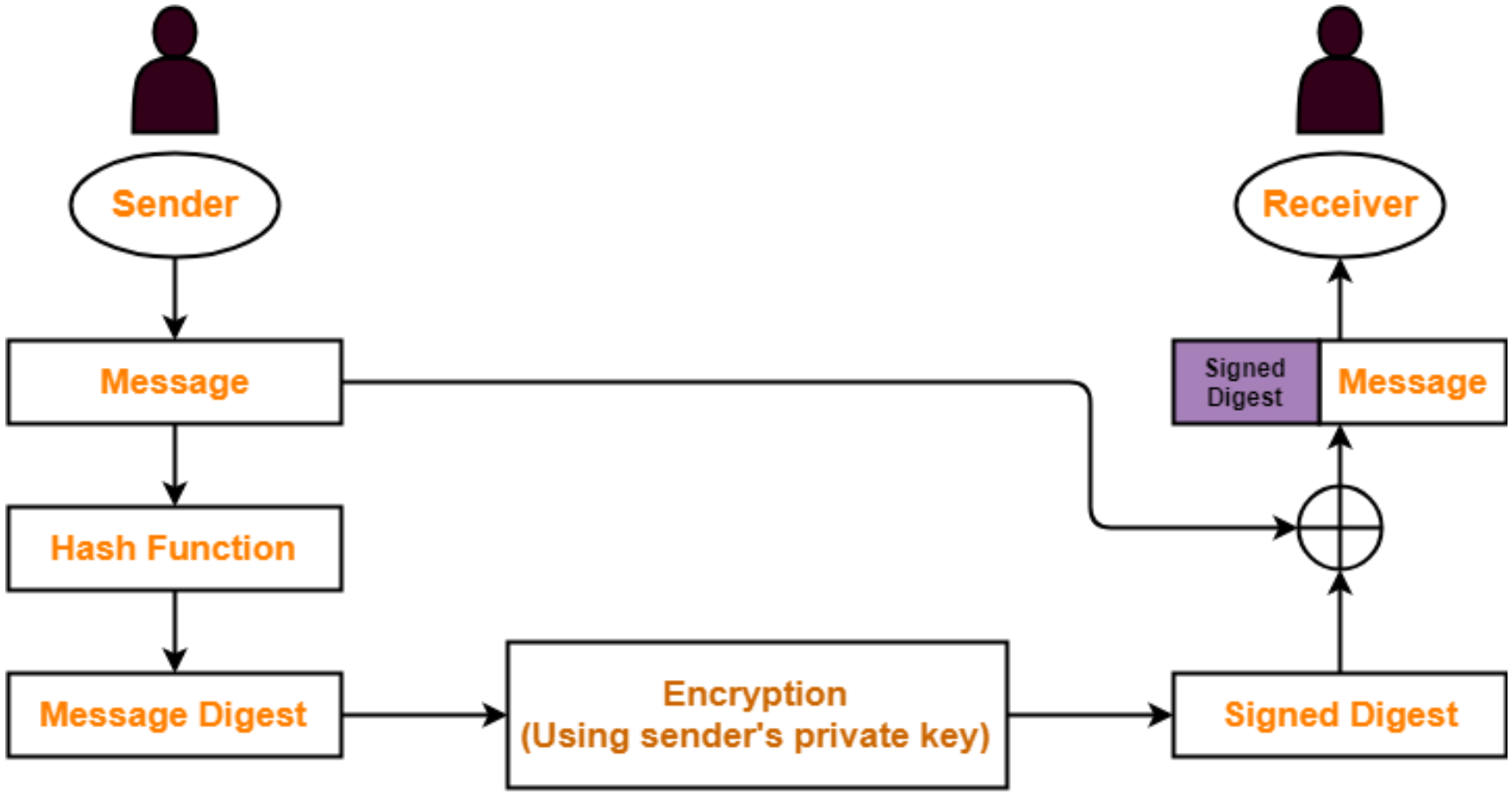
Message
Digest (MD)

?
=

Message

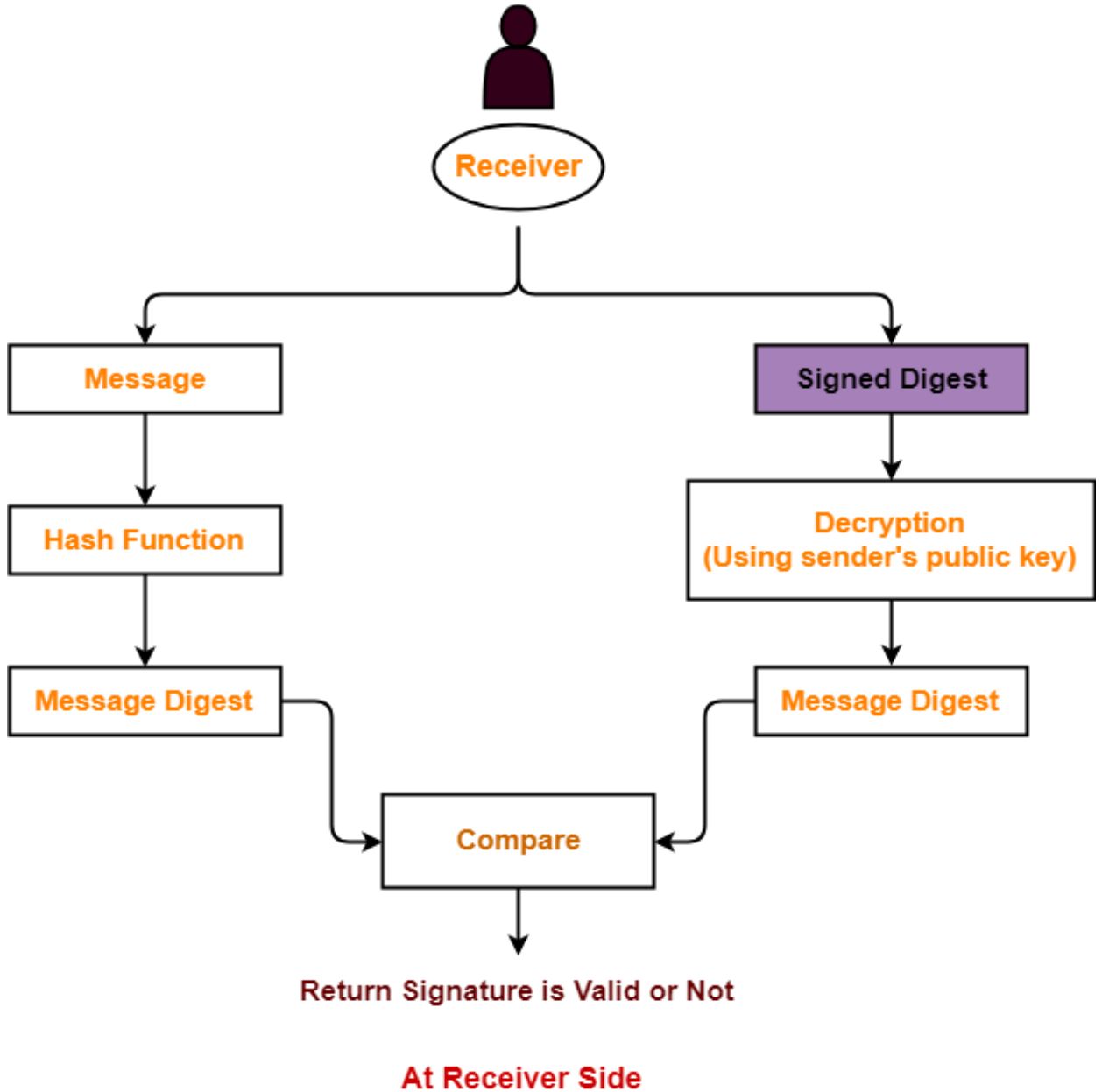
Fungsi
Hash

Message
Digest (MD')

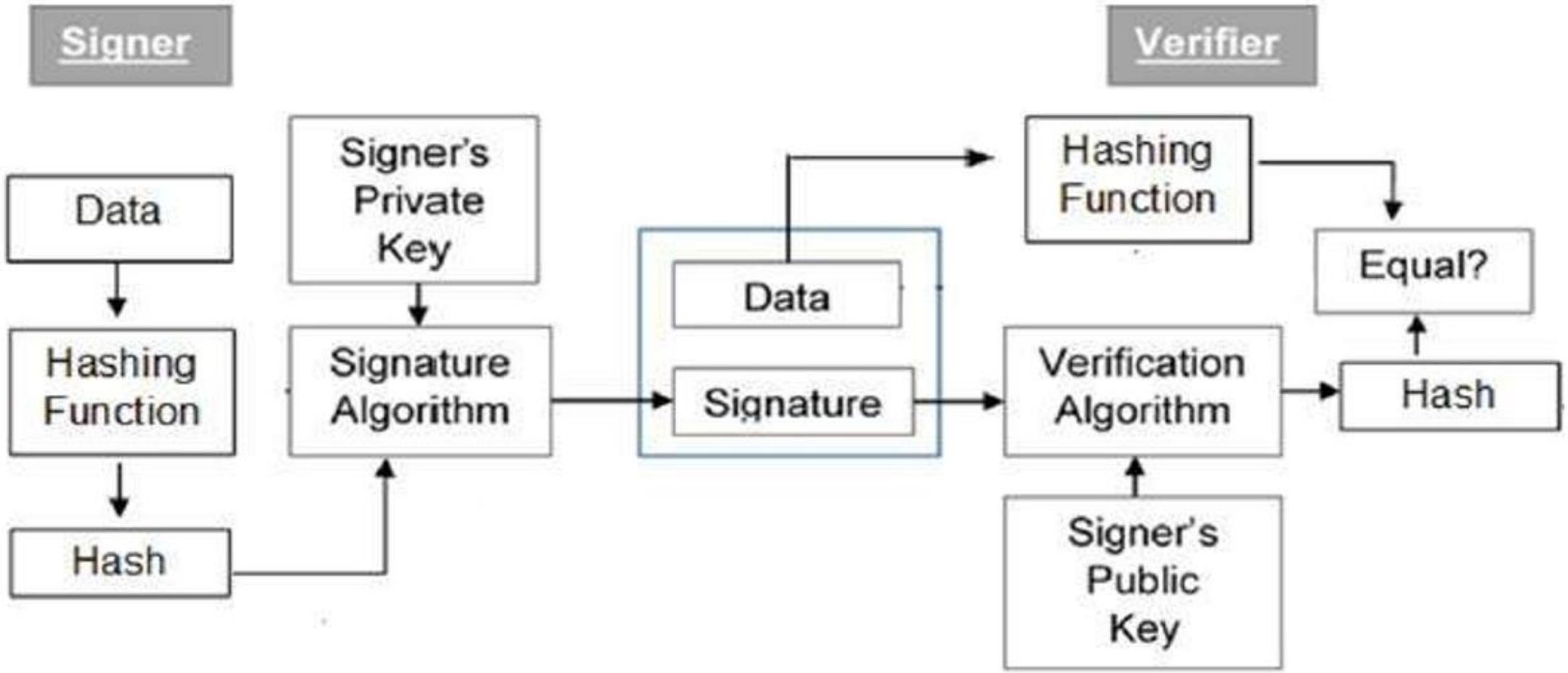


At Sender Side

https://www.gatevidyalay.com/how-digital-signature-works-algorithm/



https://www.gatevidyalay.com/how-digital-signature-works-algorithm/



https://www.includehelp.com/cryptography/digital-signature-algorithm-dsa.aspx

Empat algoritma untuk tanda-tangan digital:

1. RSA
2. Elgamal signature
3. *Digital Signature Algorithm* (DSA)
4. *Elliptic Curve Cryptography digital signature* (ECCDS)

Tanda-tangan digital dengan algoritma RSA

Langkah-langkah pemberian tanda-tangan (*signing*)

1. Pengirim menghitung nilai *hash* dari pesan *M:*

   $h = H(M)$

2. Pengirim mengenkripsi *h* dengan kunci privatnya (*PrivK*) menggunakan persamaan enkripsi *RSA,* hasilnya adalah *signature S*:

   $S = h^{PrivK} \bmod n$ (*n* adalah modulus, $n = pq$).

3. Pengirim mentransmisikan *M* + *S* ke penerima

Langkah-langkah verifikasi tanda-tangan (*verifying*)

1. Penerima menghitung nilai *hash* dari pesan *M* yang diterima:

   $h = H(M)$

2. Penerima melakukan dekripsi terhadap tanda-tangan *S* dengan kunci publik si pengirim (*PubK*) menggunakan persamaan dekripsi *RSA*:

   $h' = S^{PubK} \bmod n$

3. Penerima membandingkan *h* dengan *h'*. Jika *h* = *h'* maka tanda-tangan digital adalah otentik. Jika tidak sama, maka tanda-tangan tidak otentik sehingga pesan dianggap tidak asli lagi atau pengirimnya

Alice

M =

Pada wisuda sarjana baru ITB, ternyata ada seorang wisudawan yang paling muda. Umurnya baru 19 tahun. Ini berarti dia masuk ITB pada umur 15 tahun. Zaman sekarang banyak sarjana masih berusia muda belia. Mungkin masuk sekolah pada usia dini dan mengikuti kelas akselerasi pada tingkatan SD, SMP, dan SMA. Masuk SD umur 6 tahun dan ikut kelas aksel sehingga selesai dalam waktu lima tahun pada umur 11. SMP diselesaikan dalam waktu dua tahun dan SMA dalam waktu dua tahun, sehingga lulus SMA pada umur 15 tahun. Kuliah di ITB selama empat tahun sehingga wajar saja menjadi sarjana pada umur 19 tahun.

$h = H(M)$ = A4C05176E1440FC879C06C72FA603A24 (heksadesimal)

= 218991964599382371228554013295471770148 (desimal

$S = h^{PrivK} \bmod n$ (n = 223427, $PrivK$ = 171635)

$= (218991964599382371228554013295471770148)^{171635} \bmod (223427) = 46489$

$M + S$ =

Pada wisuda sarjana baru ITB, ternyata ada seorang wisudawan yang paling muda. Umurnya baru 19 tahun. Ini berarti dia masuk ITB pada umur 15 tahun. Zaman sekarang banyak sarjana masih berusia muda belia. Mungkin masuk sekolah pada usia dini dan mengikuti kelas akselerasi pada tingkatan SD, SMP, dan SMA. Masuk SD umur 6 tahun dan ikut kelas aksel sehingga selesai dalam waktu lima tahun pada umur 11. SMP diselesaikan dalam waktu dua tahun dan SMA dalam waktu dua tahun, sehingga lulus SMA pada umur 15 tahun. Kuliah di ITB selama empat tahun sehingga wajar saja menjadi sarjana pada umur 19 tahun.

46489

Bob

Pada wisuda sarjana baru ITB, ternyata ada seorang wisudawan yang paling muda. Umurnya baru 19 tahun. Ini berarti dia masuk ITB pada umur 15 tahun. Zaman sekarang banyak sarjana masih berusia muda belia. Mungkin masuk sekolah pada usia dini dan mengikuti kelas akselerasi pada tingkatan SD, SMP, dan SMA. Masuk SD umur 6 tahun dan ikut kelas aksel sehingga selesai dalam waktu lima tahun pada umur 11. SMP diselesaikan dalam waktu dua tahun dan SMA dalam waktu dua tahun, sehingga lulus SMA pada umur 15 tahun. Kuliah di ITB selama empat tahun sehingga wajar saja menjadi sarjana pada umur 19 tahun.
46489

$h = H(M) = \text{A4C05176E1440FC879C06C72FA603A24}$ (heksadesimal)

$= 218991964599382371228554013295471770148$ (decimal)

$\equiv 125468 \pmod{223427}$

$h' = S^{PubK} \bmod n \quad (PubK = 731)$

$= (46489)^{731} \bmod (223427)$

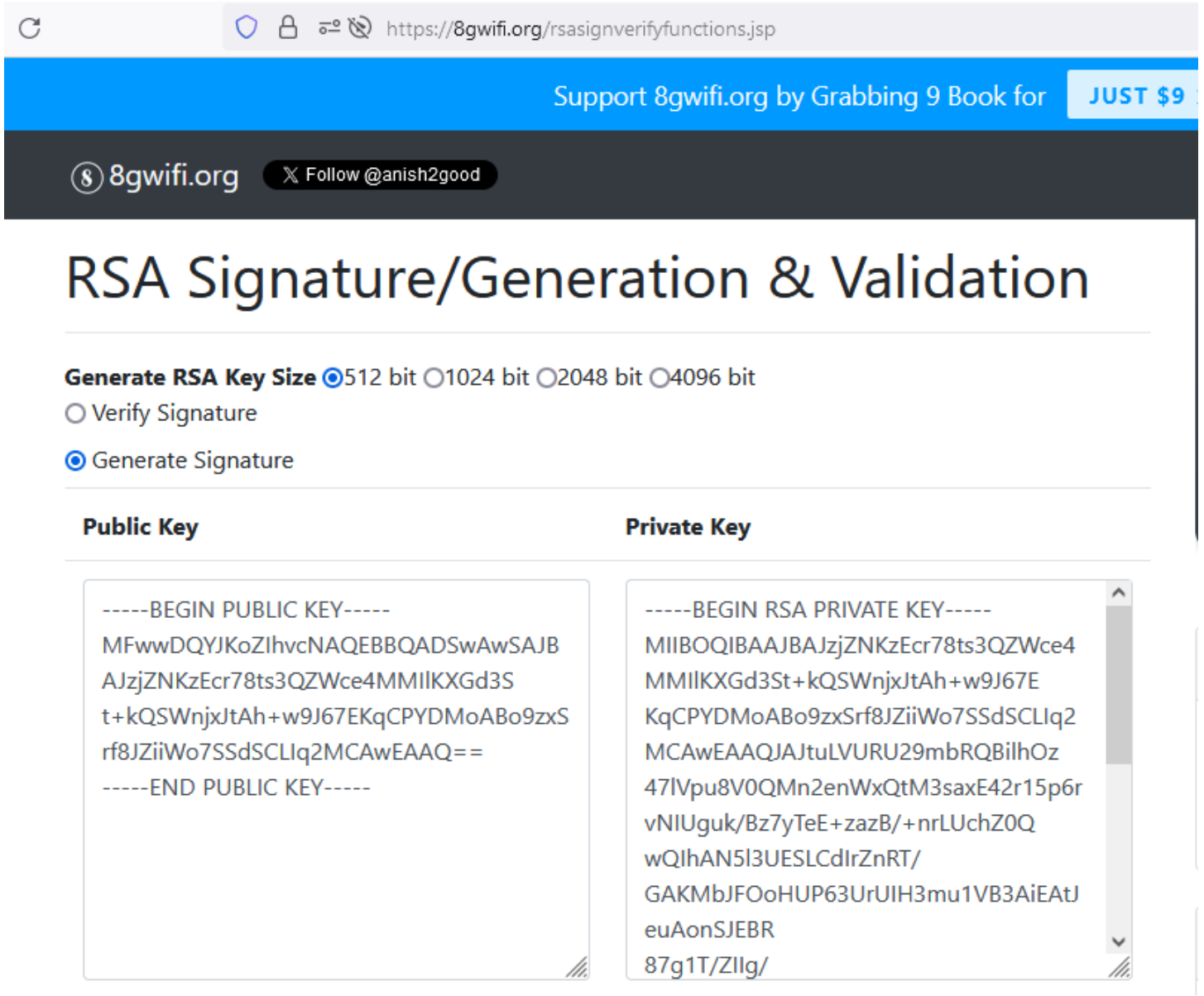
$= 125468$

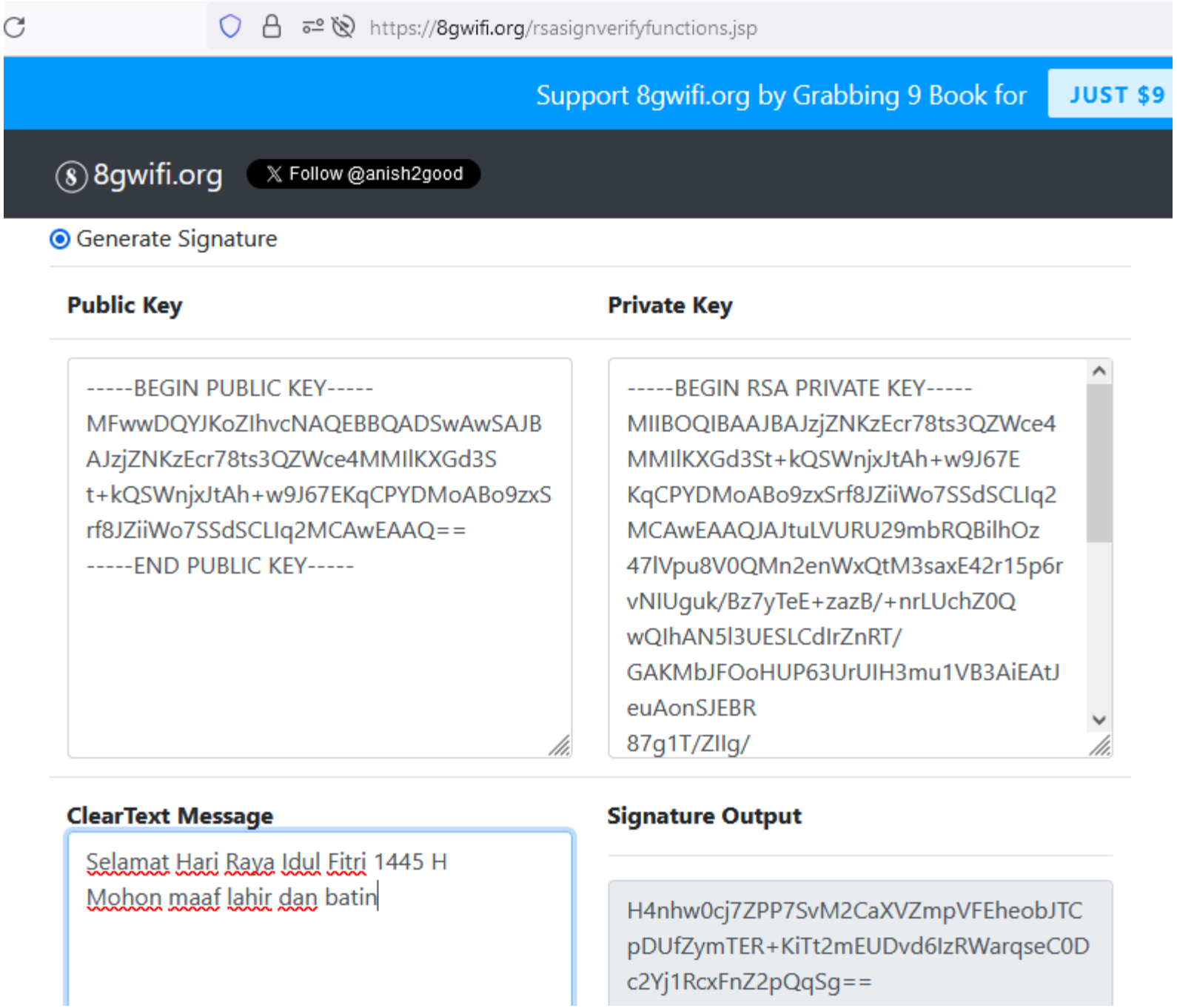
sama

Tandda tangan valid!

Demo calculator digital signature online dengan RSA

https://8gwifi.org/rsasignverifyfunctions.jsp




https://8gwifi.org/rsasignverifyfunctions.jsp
Support 8gwifi.org by Grabbing 9 Book for
JUST $9
8gwifi.org
Follow @anish2good
Generate Signature
Public Key
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
AJzjZNKzEcr78ts3QZWce4MMIlKXGd3S
t+kQSWnjxJtAh+w9J67EKqCPYDMoABo9zxS
rf8JZiiWo7SSdSCLIq2MCAwEAAQ==
-----END PUBLIC KEY-----
Private Key
-----BEGIN RSA PRIVATE KEY-----
MIIBOQIBAAJBAJzjZNKzEcr78ts3QZWce4
MMIlKXGd3St+kQSWnjxJtAh+w9J67E
KqCPYDMoABo9zxSrf8JZiiWo7SSdSCLIq2
MCAwEAAQJAJtuLVURU29mbRQBilhOz
47lVpu8V0QMn2enWxQtM3saxE42r15p6r
vNIUguk/Bz7yTeE+zazB/+nrLUchZ0Q
wQIhAN5l3UESLCdIrZnRT/
GAKMbJFOoHUP63UrUIH3mu1VB3AiEAtJ
euAonSJEBR
87g1T/ZIIg/
ClearText Message
Selamat Hari Raya Idul Fitri 1445 H
Mohon maaf lahir dan batin
Signature Output
H4nhw0cj7ZPP7SvM2CaXVZmpVFEheobJTC
pDUfZymTER+KiTt2mEUDvd6IzRWarqseC0D
c2Yj1RcxFnZ2pQqSg==


https://8gwifi.org/rsasignverifyfunctions.jsp
Support 8gwifi.org by Grabbing 9 Book for
8gwifi.org
Follow @anish2good
ClearText Message
Selamat Hari Raya Idul Fitri 1445 H
Mohon maaf lahir dan batin
Signature Output
Signature Verification Passed
Provide Signature Value (Base64)
H4nhw0cj7ZPP7SvM2CaXVZmpVFEheobJTC
pDUfZymTER+KiTt2mEUDvd6IzRWarqseC0D
c2Yj1RcxFnZ2pQqSg==

1445 H diubah menjadi 1446 H

ClearText Message

Selamat Hari Raya Idul Fitri 1446 H
Mohon maaf lahir dan batin

Signature Output

Signature Verification Failed

Provide Signature Value (Base64)

H4nhw0cj7ZPP7SvM2CaXVZmpVFEheobJTC
pDUfZymTER+KiTt2mEUDvd6IzRWarqseC0D
c2Yj1RcxFnZ2pQqSg==

Latihan 1

1. Buka situs https://8gwifi.org/rsasignverifyfunctions.jsp untuk menandatangani pesan dengan algoritma SHA1 + RSA.
2. Buatlah kunci publik dan kunci privat sepanjang 512 bit
3. Ketikkan sembarang pesan, lalu tandantangi pesan dengan menggunakan kunci privatmu.
4. Kirim kunci publik kepada temanmu via Line
5. Kirim pesan dan tanda-tangan digital kepada temanmu via Line atau email
6. Temanmu membaca pesan tersebut, *copy*, dan *paste* pesan dan tanda-tangan digital ke situs tersebut
7. Temanmu memverifikasi tanda-tangan digital dengan kunci publikmu lalu menyimpulkan apakah pesan masih asli dan berasal dari pengirim yang sebenarnya

Latihan 2

1. Buka situs https://8gwifi.org/rsasignverifyfunctions.jsp untuk menandatangani pesan dengan algoritma SHA256 + RSA.
2. Buatlah kunci publik dan kunci privat sepanjang 1024 bit
3. Buatlah sebuah surat dengan Notepad, akhiri dengan tanda pagar (#) untuk menandakan akhir surat (lihat contoh pada halaman berikut, isi bebas).
4. Copas isi surat dari Notepad ke situs, lalu bangkitkan tanda-tangan digital.
5. Copas tanda-tangan digital pada akir surat. Simpan file surat dengan nama surat.txt
6. Kirim kunci publik kepada temanmu via Line
7. Kirim surat.txt kepada temanmu via Line

8. Temanmu membaca pesan tersebut, *copy*, dan *paste* pesan (sampai tanda #) dan tanda-tangan digital ke situs tersebut
9. Temanmu memverifikasi tanda-tangan digital lalu menyimpulkan apakah pesan masih asli dan berasal dari pengirim yang sebenarnya

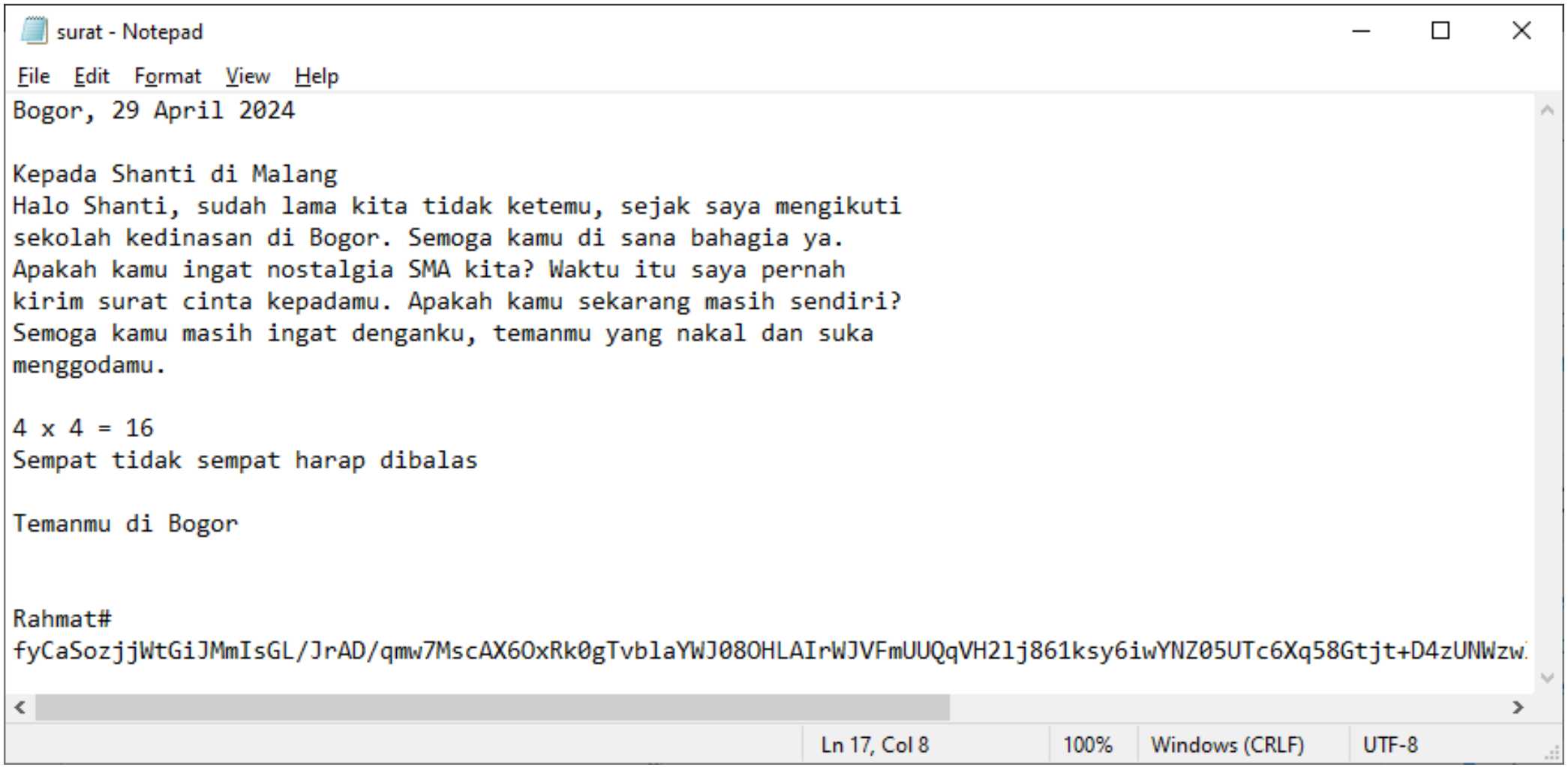
Bogor, 29 April 2024

Kepada Shanti di Malang
Halo Shanti, sudah lama kita tidak ketemu, sejak saya mengikuti sekolah kedinasan di Bogor. Semoga kamu di sana bahagia ya.
Apakah kamu ingat nostalgia SMA kita? Waktu itu saya pernah kirim surat cinta kepadamu. Apakah kamu sekarang masih sendiri?
Semoga kamu masih ingat denganku, temanmu yang nakal dan suka
menggodamu.

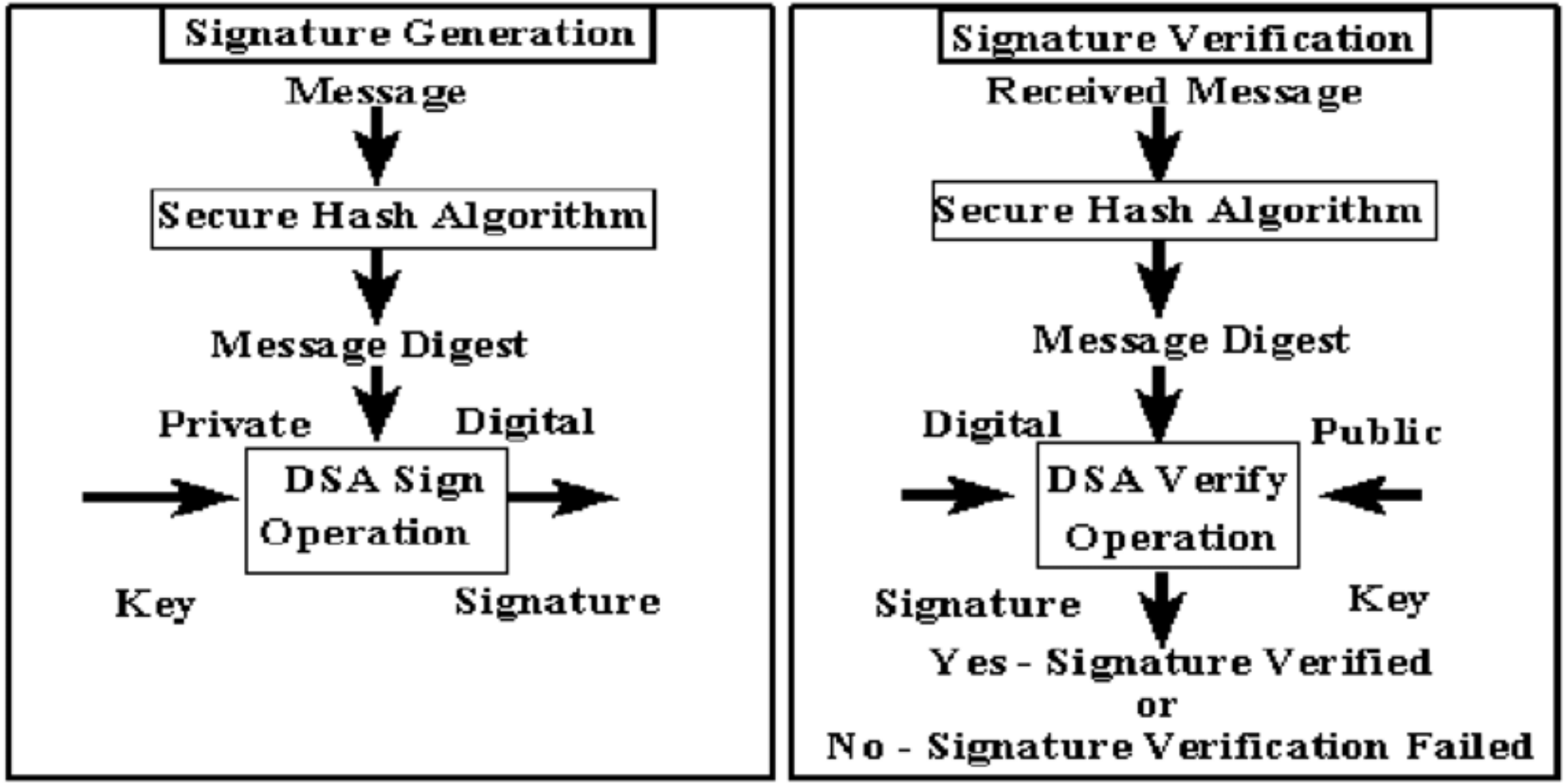
4 x 4 = 16
Sempat tidak sempat harap dibalas

Temanmu di Bogor

Rahmat#

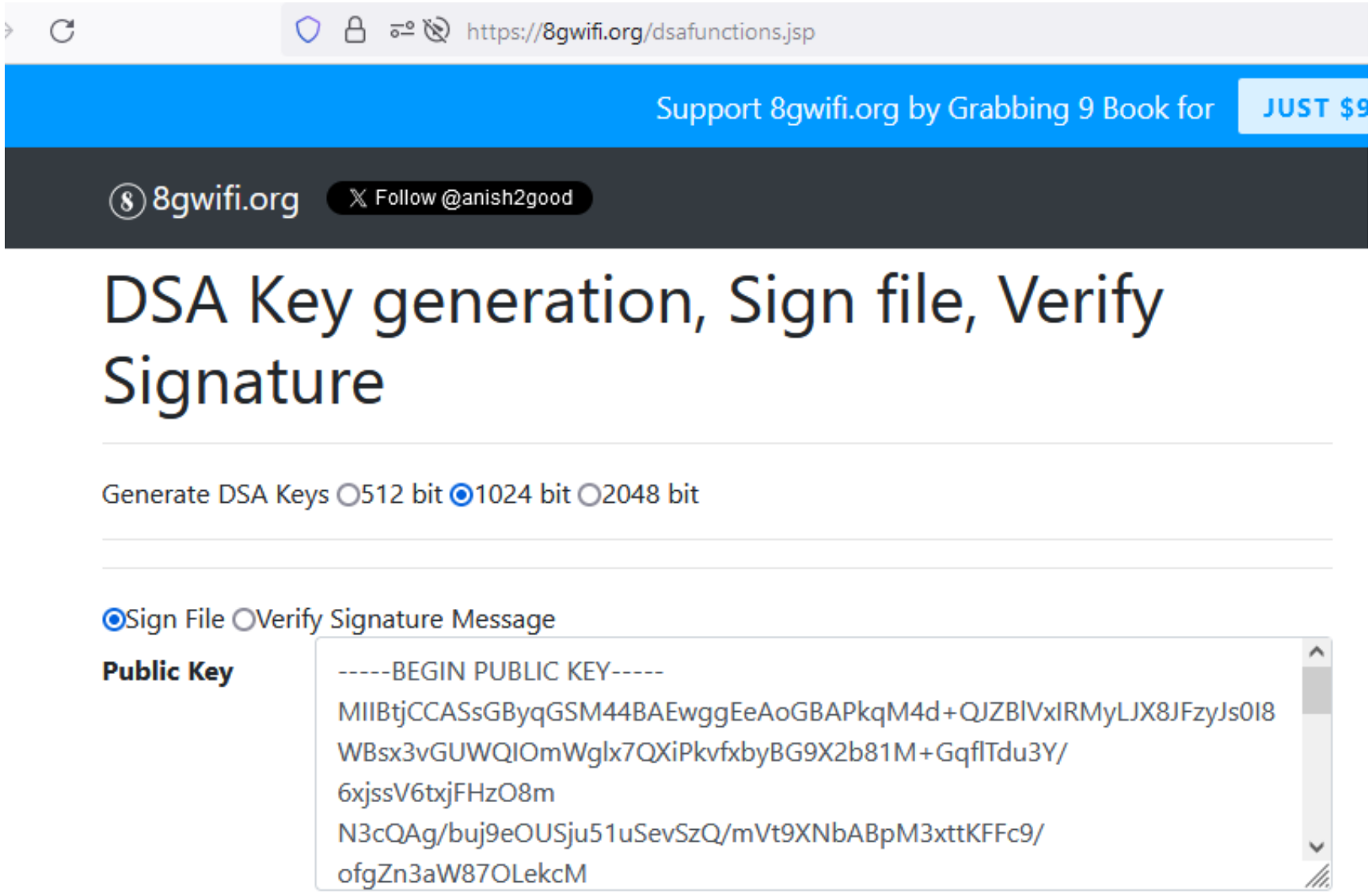

surat - Notepad
File Edit Format View Help
Bogor, 29 April 2024
Kepada Shanti di Malang
Halo Shanti, sudah lama kita tidak ketemu, sejak saya mengikuti
sekolah kedinasan di Bogor. Semoga kamu di sana bahagia ya.
Apakah kamu ingat nostalgia SMA kita? Waktu itu saya pernah
kirim surat cinta kepadamu. Apakah kamu sekarang masih sendiri?
Semoga kamu masih ingat denganku, temanmu yang nakal dan suka
menggodamu.
4 x 4 = 16
Sempat tidak sempat harap dibalas
Temanmu di Bogor
Rahmat#
fyCaSozjjWtGiJMmIsGL/JrAD/qmw7MscAX6OxRk0gTvblaYWJ08OHLAIrWJVFmUUQqVH2lj861ksy6iwYNZ05UTc6Xq58Gtjt+D4zUNWzw
Ln 17, Col 8
100%
Windows (CRLF)
UTF-8

Digital Signature Algorithm (DSA)

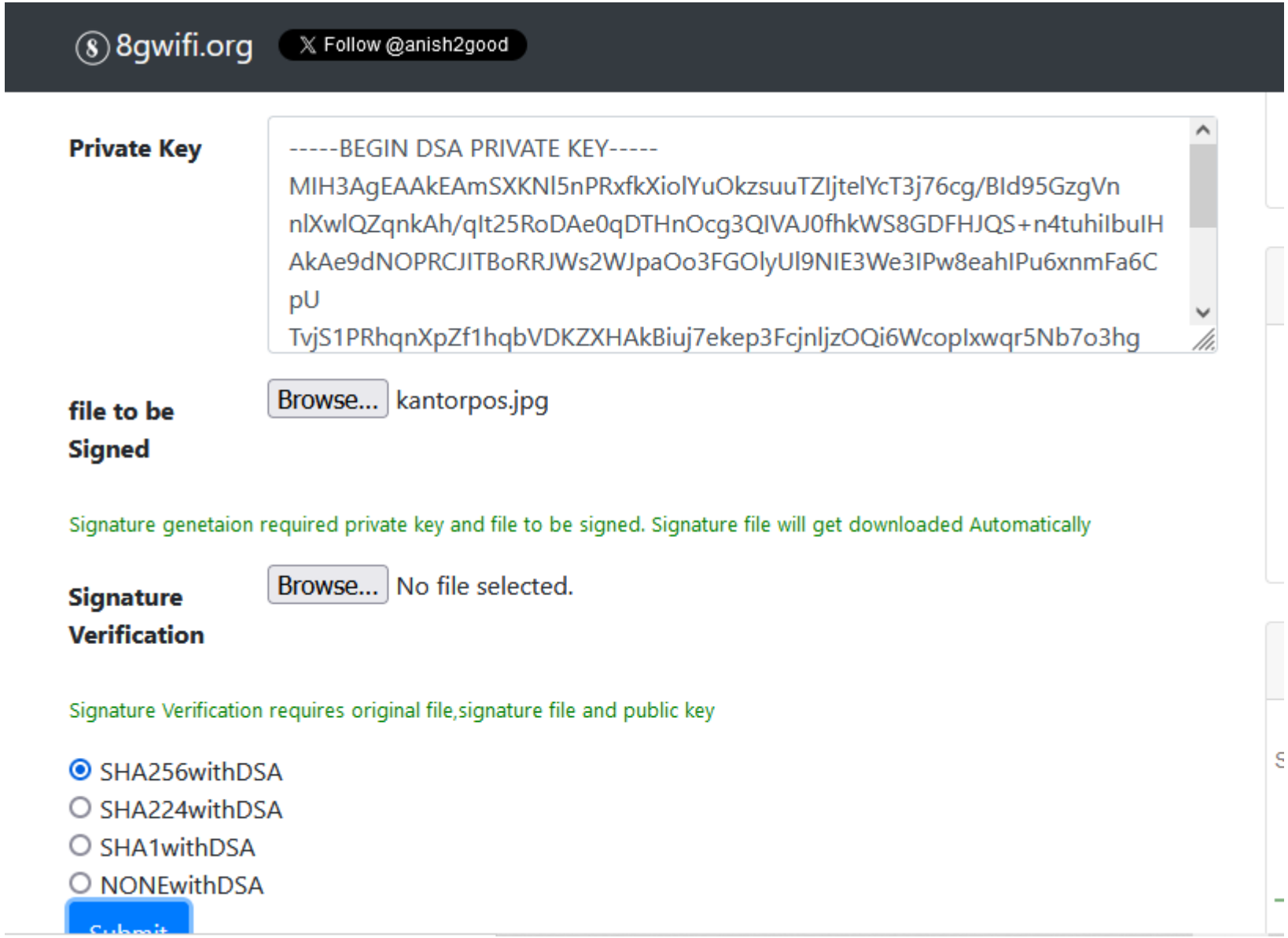


Tanda-tangan digital untuk *file* dengan DSA (*Digital Signature Algorithm*)

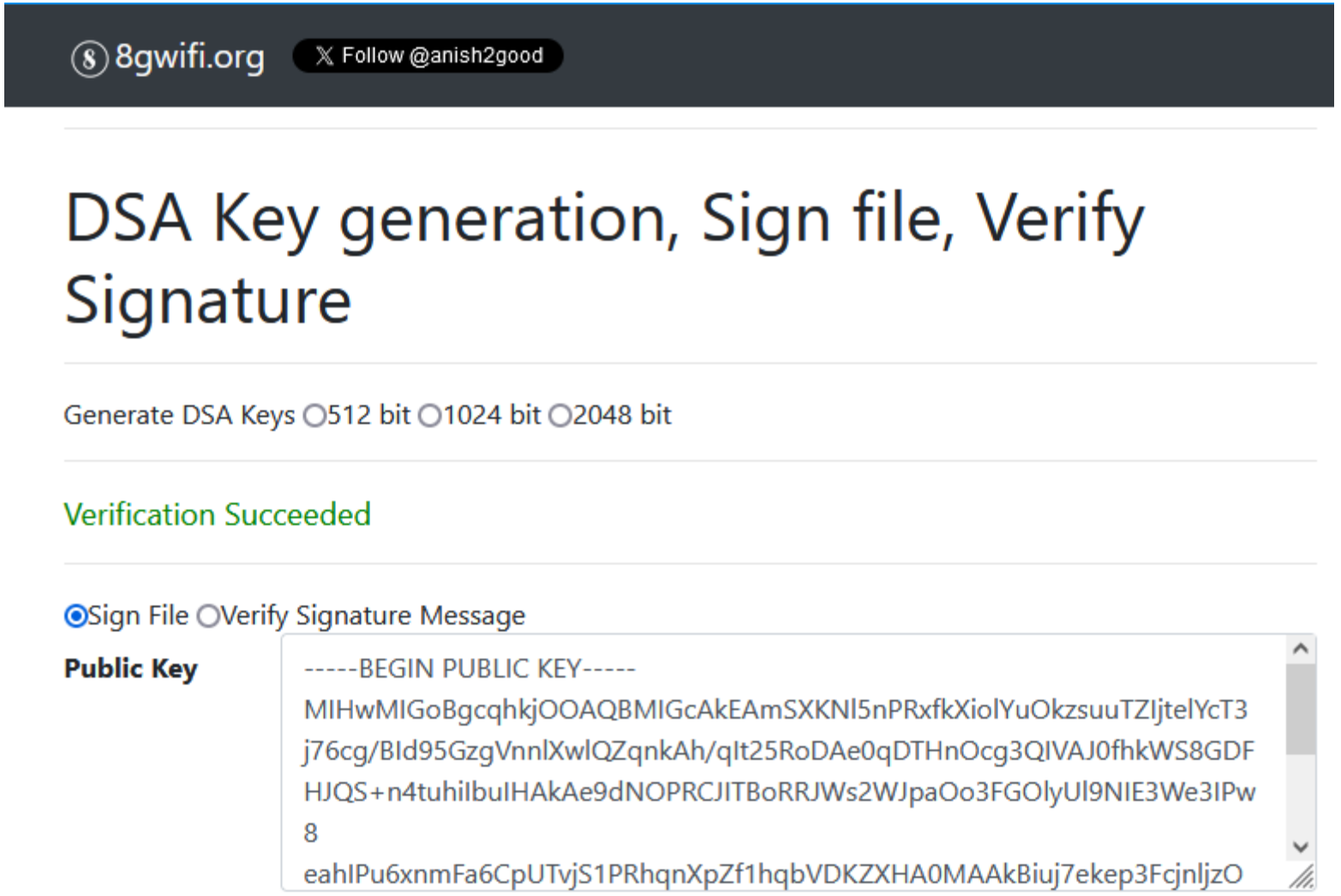
https://8gwifi.org/dsafunctions.jsp



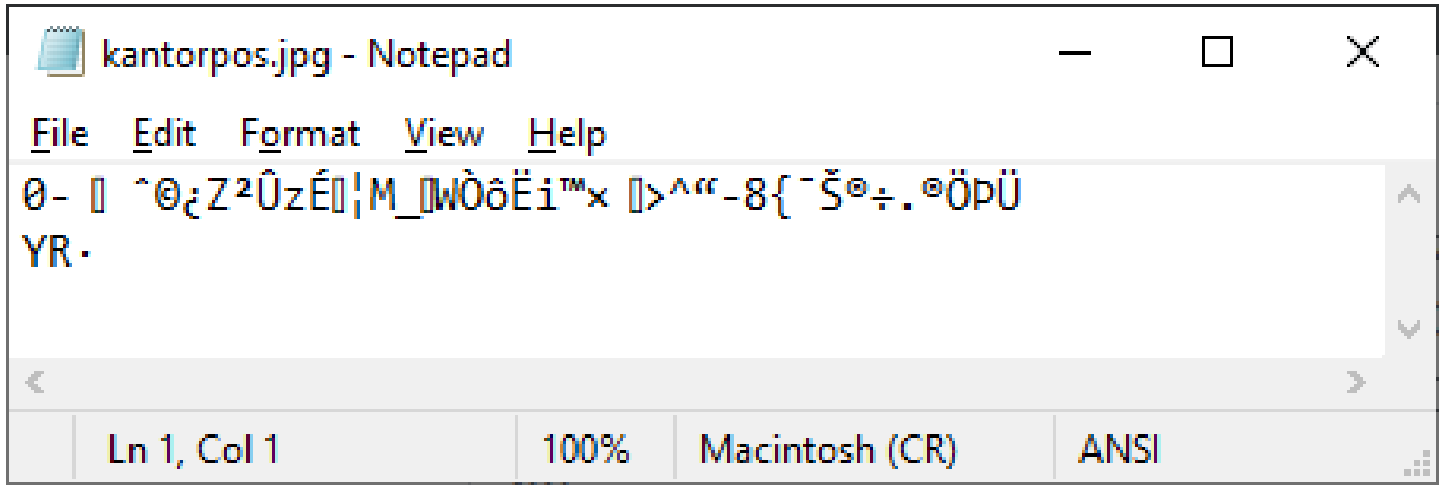
- File yang akan ditanda-tangani: kantor-pos.jpg


8gwifi.org
Follow @anish2good
Private Key
-----BEGIN DSA PRIVATE KEY-----
MIH3AgEAAkEAmSXKNl5nPRxfkXiolYuOkzsuuTZIjtelYcT3j76cg/BId95GzgVn
nlXwlQZqnkAh/qIt25RoDAe0qDTHnOcg3QIVAJ0fhkWS8GDFHJQS+n4tuhiIbuIH
AkAe9dNOPRCJITBoRRJWs2WJpaOo3FGOlyUl9NIE3We3IPw8eahIPu6xnmFa6C
pU
TvjS1PRhqnXpZf1hqbVDKZXHAkBiuj7ekep3FcjnljzOQi6WcopIxwqr5Nb7o3hg
file to be Signed
Browse...
kantorpos.jpg
Signature genetaion required private key and file to be signed. Signature file will get downloaded Automatically
Signature Verification
Browse...
No file selected.
Signature Verification requires original file,signature file and public key
SHA256withDSA
SHA224withDSA
SHA1withDSA
NONEwithDSA

- Verifikasi tanda-tangan digital:



Tanda-tangan digital yang dihasilkan:



Latihan 3

1. Buka situs https://8gwifi.org/dsafunctions.jsp untuk menandatangani pesan dengan algoritma SHA1 + DSA.
2. Buatlah kunci publik dan kunci privat sepanjang 1024 bit
3. Unggah sebuah file (bebas, file gambar, file docx, file excel, dll).
4. Tanda-tangani file dengan kunci privatmu
5. Simpan tanda-tangan digital
6. Unggah Kembali tanda-tangan digital
7. Ubah file dengan aplikasi (Word, Paint, dsb), simpan.
8. Verifikasi tanda-tangan digital dengan menggunakan kunci public.

SELAMAT BELAJAR