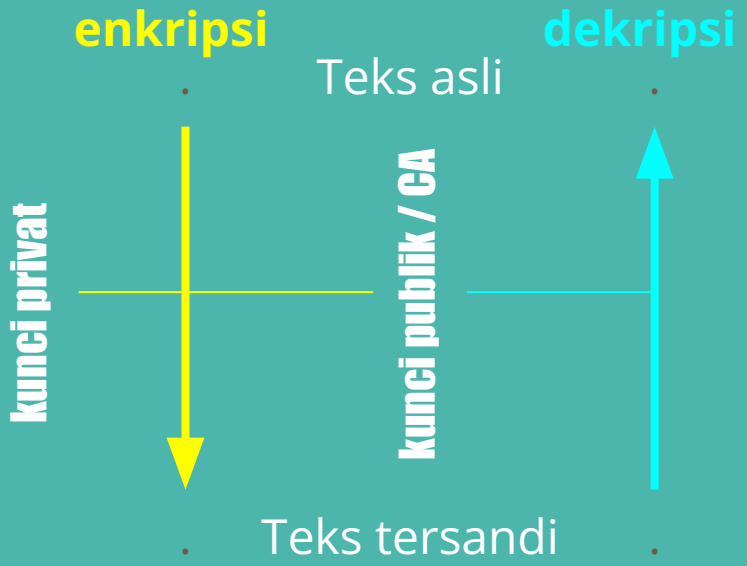
Application Signing

Mobile Security
Magister Informatika (MiT)
Universitas Ahmad Dahlan

Kriptografi: Enkripsi Asimetris

Signing Basic I

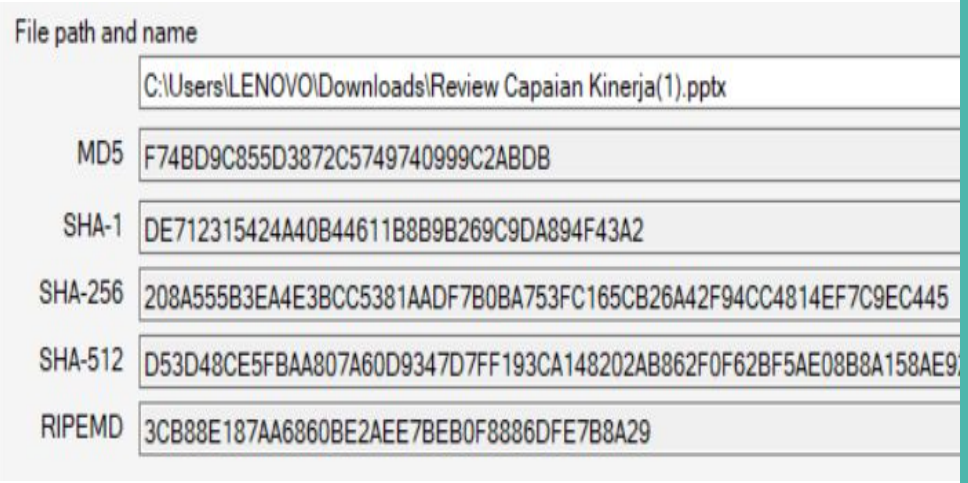


- Dapat diberikan **password** pada kunci privat. Dapat ditambahkan **salt** dan **pepper**
- Contoh algoritma: RSA, DSA

https://bptsi.unisayogya.ac.id/certificate-authority-digital-signature-dan-certificate-revocation-list-crl/
https://bptsi.unisayogya.ac.id/memperkuat-general-purpose-hashing/

Hash:
General Purpose Hash

Signing Basic II



https://bptsi.unisayogya.ac.id/general-purpose-hashing-vs-password-hashing/

- Representasi data ke dalam string dengan jumlah karakter tetap, misalnya md5 memiliki panjang string 32
- Memungkinkan terjadi tabrakan
- Hash (**1 way**) vs Encrypt (2 way)
- General purpose hash (**cepat**) vs Password hash (lambat)
- Dapat digunakan untuk **checksum**, dapat menggunakan beberapa algoritma
- Contoh algoritma: md-family, sha-family

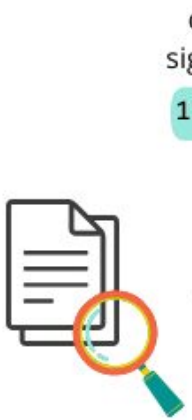
Digital Signature

Signing Basic III

https://bptsi.unisayogya.ac.id/tanda-tangan-elektronik-tte-mandiri/2/#ttd-berkas-ssl
https://bptsi.unisayogya.ac.id/certificate-authority-digital-signature-dan-certificate-revocation-list-crl/

- melakukan **hash** terhadap dokumen
- informasi-informasi (termasuk hash) di-enkripsi dengan **kunci privat dan kunci publik/CA**
- melekatkan/menyisipkan (**embed**) ke dalam dokumen

Penandatanganan



digital signature: `1111...`

konten asli: `0110110101010101...`

enkripsi

hash ( ) = abc123
informasi 1
...
informasi n

`1111111000000...`

kunci privat

Verifikasi

digital signature: `1111...`

konten asli: `0110110101010101...`

dekripsi

hash ( ) = abc123

jika sama, maka valid

hash = abc123
informasi 1
...
informasi n

`1000000111111...`

kunci publik

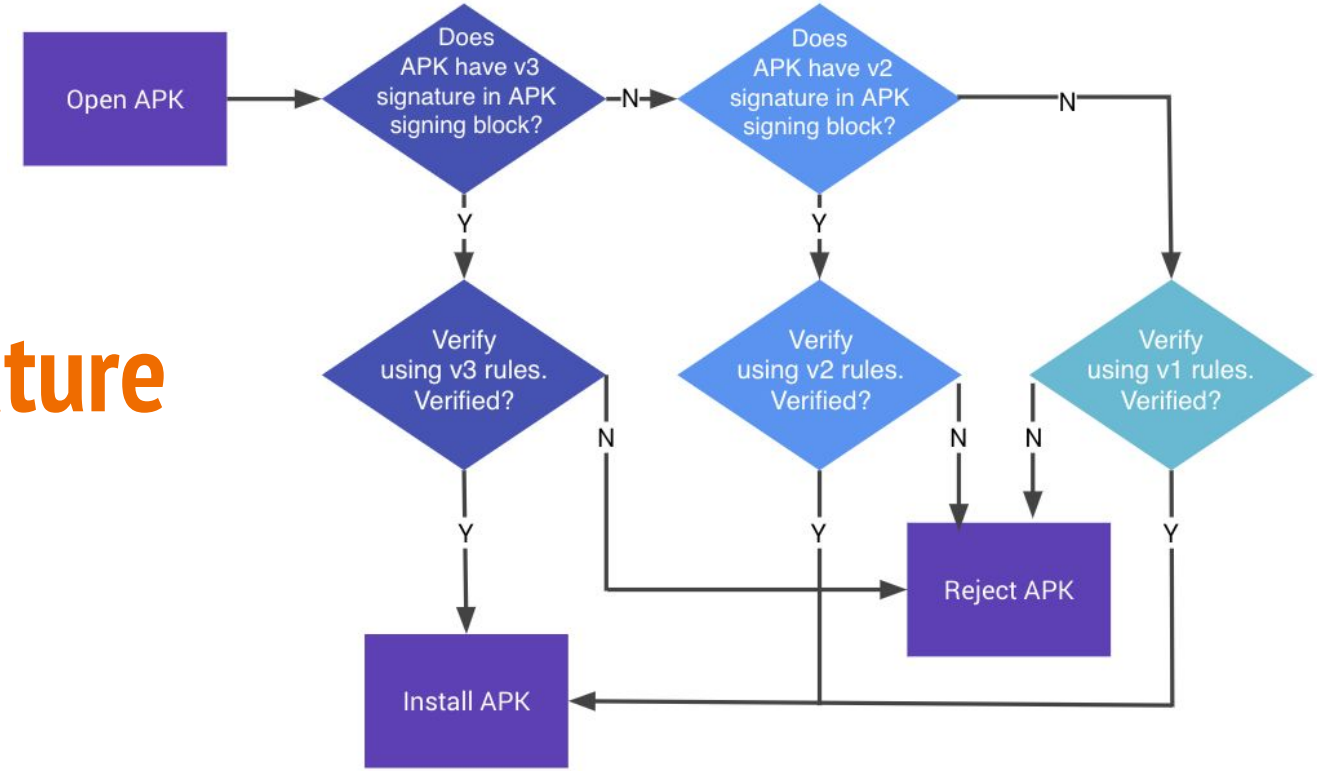
(opsional)
dapat menambahkan:

untuk interoperabilitas
umumnya tidak menggunakan
salt dan/atau pepper

ilustrasi hash
hash(0110110101010101) = be2824848e53fe2e2d6015ff68ee7072
hash(0110110101010100) = 731d1ffc634f4e5ac44b01592b12a0ad

APK Signature

Brief



APK Signature

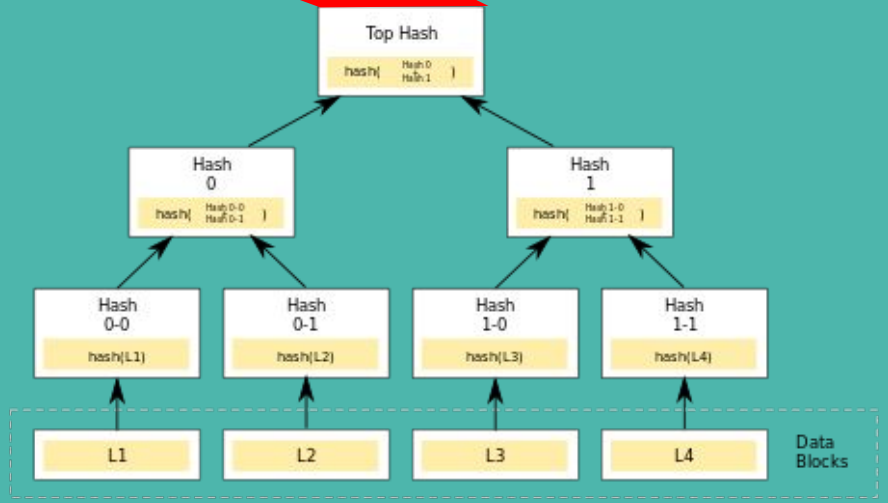
Scheme v1

- Hanya menandatangani jar
- Bagian lain, seperti metadata ZIP, tidak ditandatangani
- Verifikasi:
  isi harus sama dengan yang tercantum di META-INF/MANIFEST.MF dan ditandatangani dengan set penandatangan yang sama

https://source.android.com/docs/security/features/apksigning?hl=id

APK Signature

Scheme v2 (part 1)



Merkle tree

https://source.android.com/docs/security/features/apksigning/v2?hl=id

APK Signature

Scheme v2 (part 2)

- [bag. 1] *signed data*: data berupa id algoritma (beberapa + salt), digest, sertifikat X.509, dan atribut tambahan ditandatangani secara digital; [bag. 2] data berisi id algoritma dan tanda tangan dari *signed data;* [bag. 3] kunci publik
- Verifikasi:
  - verifikasi blok dan temukan blok skema sesuai versi
  - digest [bag. 1] = digest [bag. 2], didekripsi dengan [bag. 3]; urutan id algoritma [bag. 1] = [bag. 2]
  - hash konten apk = digest [bag. 1]
  - sertifikat X.509 [bag. 1] identik dengan [bag. 3]

APK Signature

Scheme v3

- = scheme v2
- + versi SDK yang didukung
- + struktur proof-of-rotation

https://source.android.com/docs/security/features/apksigning/v3?hl=id