Aakash R
CB.SC.P2CYS23011

Key store and Key signing:

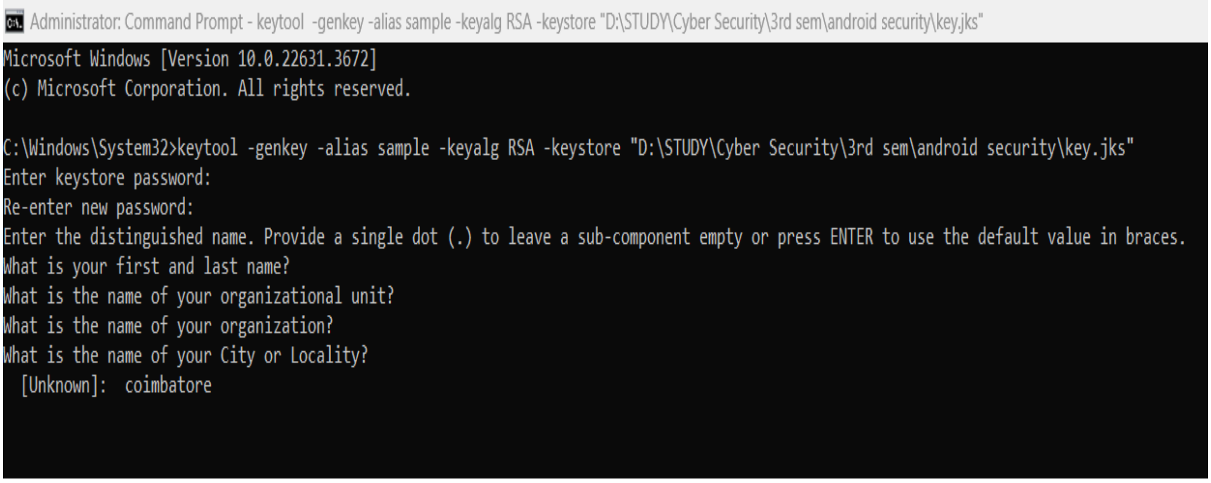
The Android Keystore and key signing are essential components in ensuring the security and integrity of Android applications.

The **Android Keystore System** allows developers to securely store cryptographic keys in a way that makes them less susceptible to extraction and misuse.

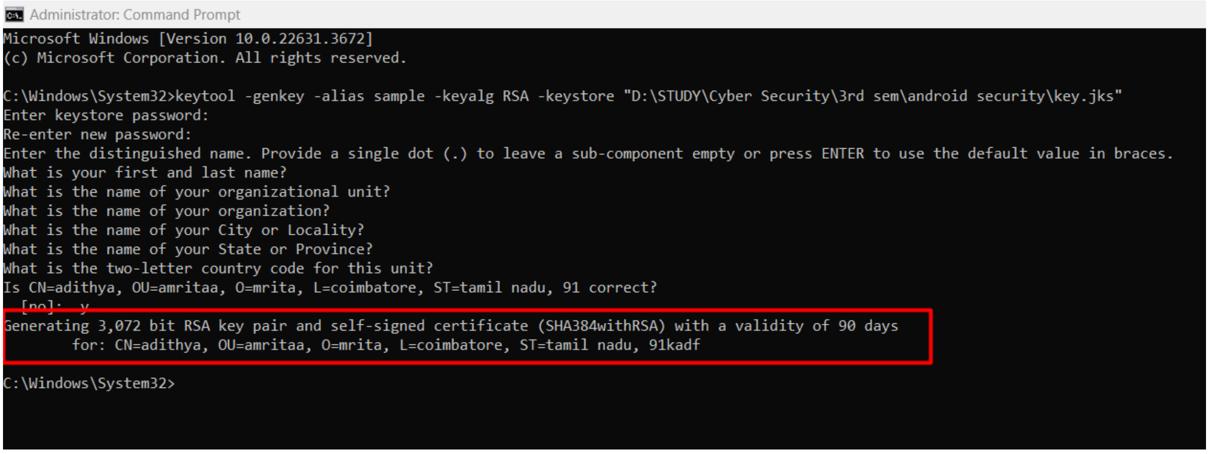
Common Operations

- Generating Keys: You can generate asymmetric (RSA, EC) and symmetric (AES) keys.
- Using Keys: Keys can be used for various operations like encryption, decryption, signing, and verification.
- Storing and Retrieving Keys: Once generated, keys can be stored and later retrieved for cryptographic operations.

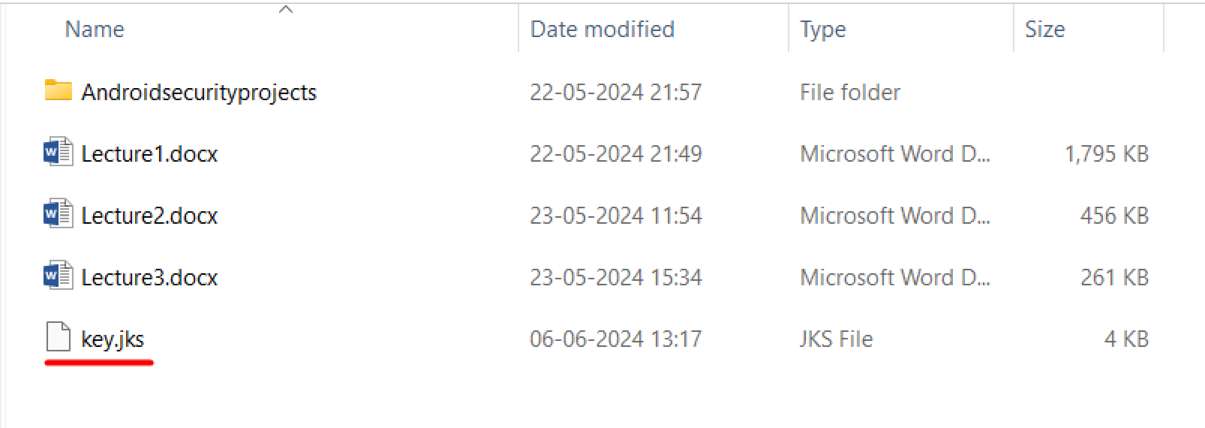
Key generation:



```
Administrator: Command Prompt - keytool  -genkey -alias sample -keyalg RSA -keystore "D:\STUDY\Cyber Security\3rd sem\android security\key.jks"
Microsoft Windows [Version 10.0.22631.3672]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>keytool -genkey -alias sample -keyalg RSA -keystore "D:\STUDY\Cyber Security\3rd sem\android security\key.jks"
Enter keystore password:
Re-enter new password:
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
  [Unknown]:  coimbatore
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3672]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>keytool -genkey -alias sample -keyalg RSA -keystore "D:\STUDY\Cyber Security\3rd sem\android security\key.jks"
Enter keystore password:
Re-enter new password:
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Is CN=adithya, OU=amritaa, O=mrita, L=coimbatore, ST=tamil nadu, 91 correct?
  [no]:  y
Generating 3,072 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 90 days
        for: CN=adithya, OU=amritaa, O=mrita, L=coimbatore, ST=tamil nadu, 91kadf

C:\Windows\System32>
```



Name	Date modified	Type	Size
Androidsecurityprojects	22-05-2024 21:57	File folder	
Lecture1.docx	22-05-2024 21:49	Microsoft Word D...	1,795 KB
Lecture2.docx	23-05-2024 11:54	Microsoft Word D...	456 KB
Lecture3.docx	23-05-2024 15:34	Microsoft Word D...	261 KB
key.jks	06-06-2024 13:17	JKS File	4 KB

Key signing is a crucial process in Android development that ensures the authenticity and integrity of an APK file. Each APK must be signed with a certificate before it can be installed on a device.

Key Components

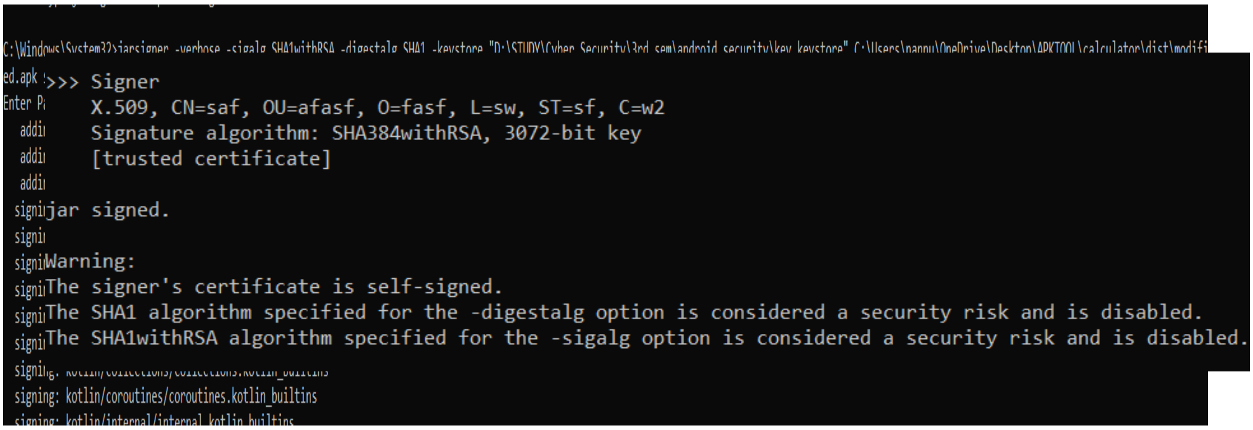
- **Signing Keys**: The private key used to sign the APK, which must be kept secure.
- **Certificates**: The public key certificate corresponding to the signing key, embedded in the APK, allows users to verify the source of the application.

Tools Used:

Jarsigner:

Used to sign Java ARchive (JAR) files, including APKs.

Signs the APK file using the private key from the keystore.



```
C:\Windows\System32>jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore "D:\STUDY\Cyber Security\3rd sem\android security\key.keystore" C:\Users\nannu\OneDrive\Desktop\APKTOOL\calculator\dist\modifi
ed.apk :>>> Signer
Enter Pa      X.509, CN=saf, OU=afasf, O=fasf, L=sw, ST=sf, C=w2
   addi       Signature algorithm: SHA384withRSA, 3072-bit key
   addi       [trusted certificate]
   addi
  signijar signed.
  signi
  signiWarning:
  signiThe signer's certificate is self-signed.
  signiThe SHA1 algorithm specified for the -digestalg option is considered a security risk and is disabled.
  signiThe SHA1withRSA algorithm specified for the -sigalg option is considered a security risk and is disabled.
  signing: kotlin/collections/collections.kotlin_builtins
  signing: kotlin/coroutines/coroutines.kotlin_builtins
  signing: kotlin/internal/internal.kotlin_builtins
```

APK Signature Scheme v2 and v3

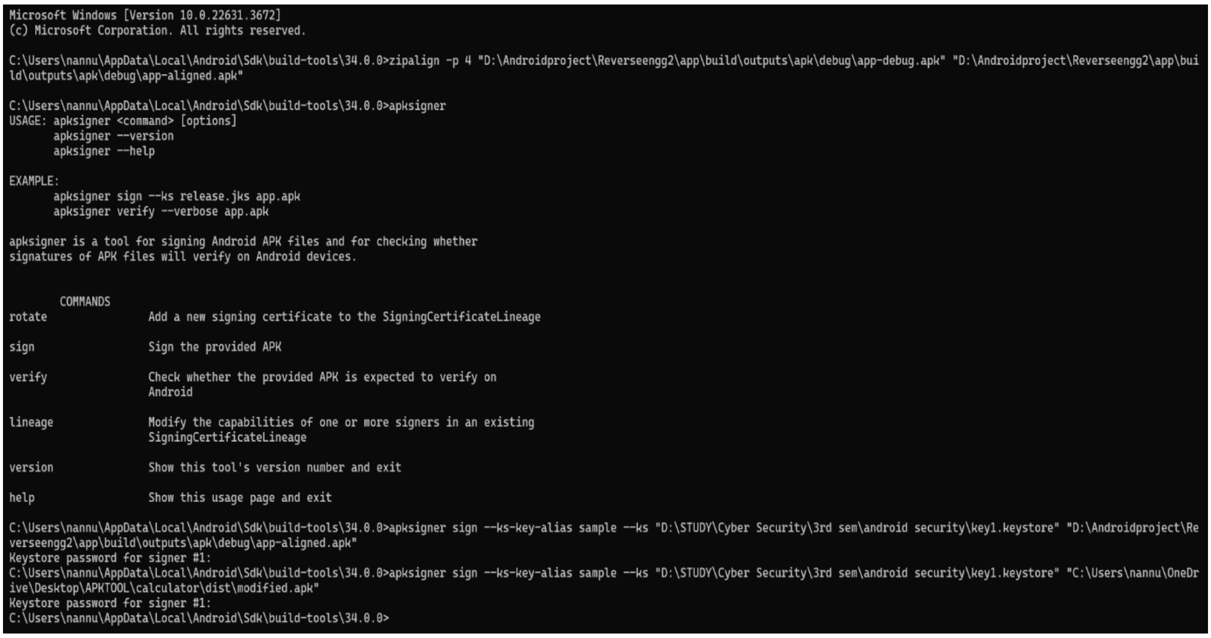
Enhances security by providing stronger guarantees that the APK hasn't been tampered with.

The newer Android versions (7.0 and above) use APK Signature Scheme v2 or v3, which offers additional protections compared to the original JAR signing.

Jarsigner:

Jarsigner can sign JAR files (which APKs are a type of) with a private key from a keystore.

It can also verify the signatures of signed JAR files, ensuring that the content hasn't been tampered with.



```
Microsoft Windows [Version 10.0.22631.3672]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nannu\AppData\Local\Android\Sdk\build-tools\34.0.0>zipalign -p 4 "D:\Androidproject\Reverseengg2\app\build\outputs\apk\debug\app-debug.apk" "D:\Androidproject\Reverseengg2\app\bui
ld\outputs\apk\debug\app-aligned.apk"

C:\Users\nannu\AppData\Local\Android\Sdk\build-tools\34.0.0>apksigner
USAGE: apksigner <command> [options]
       apksigner --version
       apksigner --help

EXAMPLE:
       apksigner sign --ks release.jks app.apk
       apksigner verify --verbose app.apk

apksigner is a tool for signing Android APK files and for checking whether
signatures of APK files will verify on Android devices.


        COMMANDS
rotate                Add a new signing certificate to the SigningCertificateLineage

sign                  Sign the provided APK

verify                Check whether the provided APK is expected to verify on
                      Android

lineage               Modify the capabilities of one or more signers in an existing
                      SigningCertificateLineage

version               Show this tool's version number and exit

help                  Show this usage page and exit

C:\Users\nannu\AppData\Local\Android\Sdk\build-tools\34.0.0>apksigner sign --ks-key-alias sample --ks "D:\STUDY\Cyber Security\3rd sem\android security\key1.keystore" "D:\Androidproject\Re
verseengg2\app\build\outputs\apk\debug\app-aligned.apk"
Keystore password for signer #1:
C:\Users\nannu\AppData\Local\Android\Sdk\build-tools\34.0.0>apksigner sign --ks-key-alias sample --ks "D:\STUDY\Cyber Security\3rd sem\android security\key1.keystore" "C:\Users\nannu\OneDr
ive\Desktop\APKTOOL\calculator\dist\modified.apk"
Keystore password for signer #1:
C:\Users\nannu\AppData\Local\Android\Sdk\build-tools\34.0.0>
```

Verifying a Signed JAR/APK File

To verify that a JAR or APK file has been correctly signed and has not been tampered with, use:

jarsigner -verify -verbose -certs my-application.apk

-verify: Indicates that the tool should verify the JAR/APK file.

-certs: Displays the certificate information used to sign the file