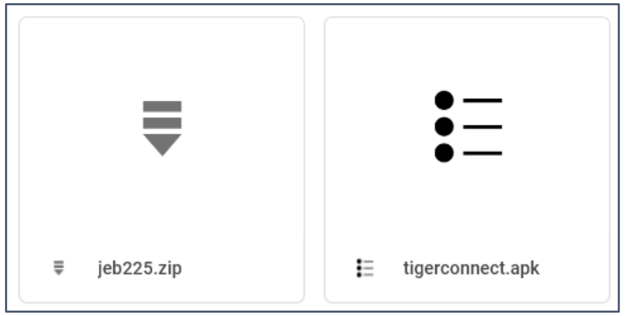
tigerconnect.apk
JEB로 앱 분석

정보보안암호수학과 20182209 김수빈

JEB 실행하기

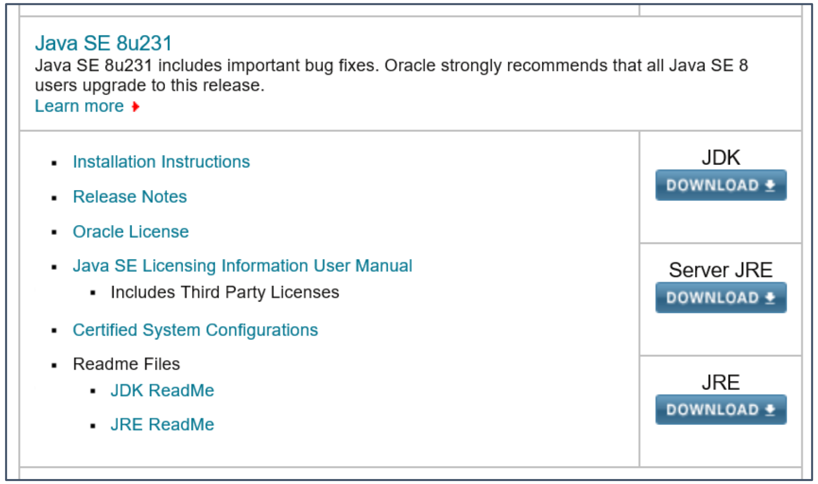
1. JEB , APK 설치



jeb225.zip

tigerconnect.apk

2. JAVA 설치



Java SE 8u231

Java SE 8u231 includes important bug fixes. Oracle strongly recommends that all Java SE 8 users upgrade to this release.

Learn more

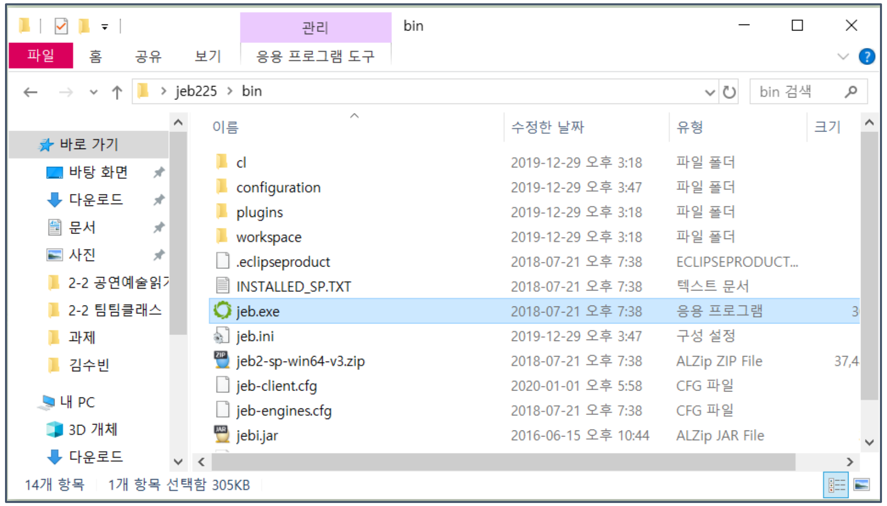
- Installation Instructions
- Release Notes
- Oracle License
- Java SE Licensing Information User Manual
  - Includes Third Party Licenses
- Certified System Configurations
- Readme Files
  - JDK ReadMe
  - JRE ReadMe

JDK

Server JRE

JRE

3. JEB 실행

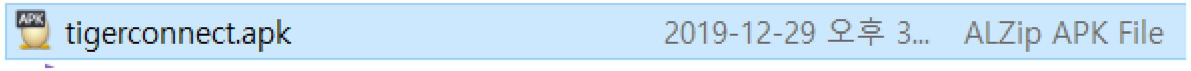


이름	수정한 날짜	유형	크기
cl	2019-12-29 오후 3:18	파일 폴더	
configuration	2019-12-29 오후 3:47	파일 폴더	
plugins	2019-12-29 오후 3:18	파일 폴더	
workspace	2019-12-29 오후 3:18	파일 폴더	
.eclipseproduct	2018-07-21 오후 7:38	ECLIPSEPRODUCT...	
INSTALLED_SP.TXT	2018-07-21 오후 7:38	텍스트 문서	
jeb.exe	2018-07-21 오후 7:38	응용 프로그램	3
jeb.ini	2019-12-29 오후 3:47	구성 설정	
jeb2-sp-win64-v3.zip	2018-07-21 오후 7:38	ALZip ZIP File	37,4
jeb-client.cfg	2020-01-01 오후 5:58	CFG 파일	
jeb-engines.cfg	2018-07-21 오후 7:38	CFG 파일	
jebi.jar	2016-06-15 오후 10:44	ALZip JAR File	

14개 항목 1개 항목 선택함 305KB

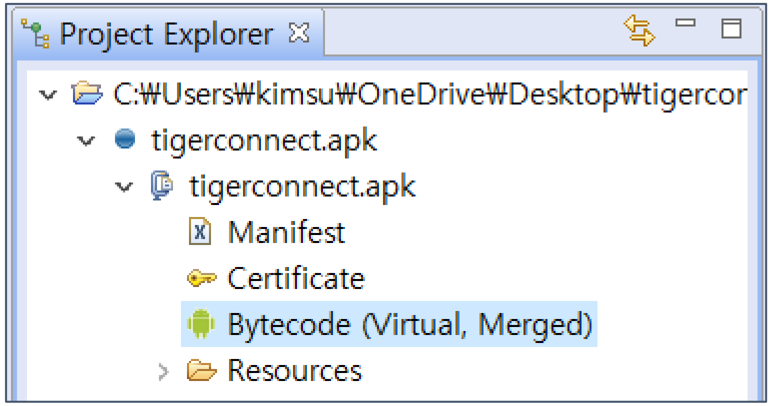
JEB 실행하기

1. 파일 – 열기 – 앱 선택



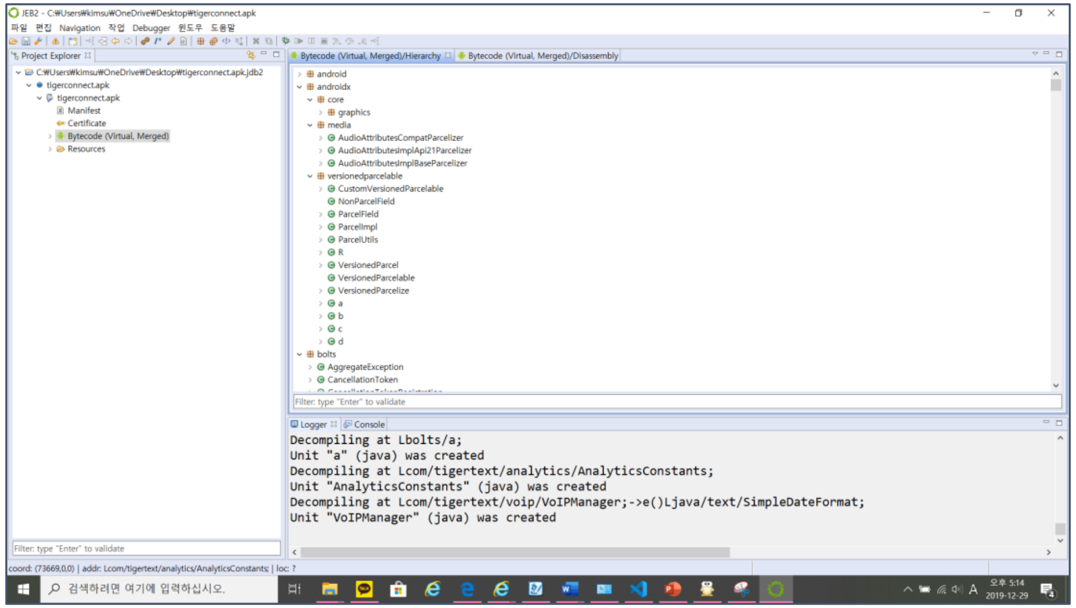
tigerconnect.apk 2019-12-29 오후 3... ALZip APK File

2. Project Explore에서 앱 더블클릭 → bytecode 더블클릭



```
C:₩Users₩kimsu₩OneDrive₩Desktop₩tigercor
  tigerconnect.apk
    tigerconnect.apk
      Manifest
      Certificate
      Bytecode (Virtual, Merged)
      Resources
```

3. classes.dex 파일 보여줌



JEB2 - C:₩Users₩kimsu₩OneDrive₩Desktop₩tigerconnect.apk
파일 편집 Navigation 작업 Debugger 윈도우 도움말
Project Explorer
Bytecode (Virtual, Merged)/Hierarchy
Bytecode (Virtual, Merged)/Disassembly
Logger
Console
Filter: type "Enter" to validate
검색하려면 여기에 입력하십시오.
오후 5:14
2019-12-29

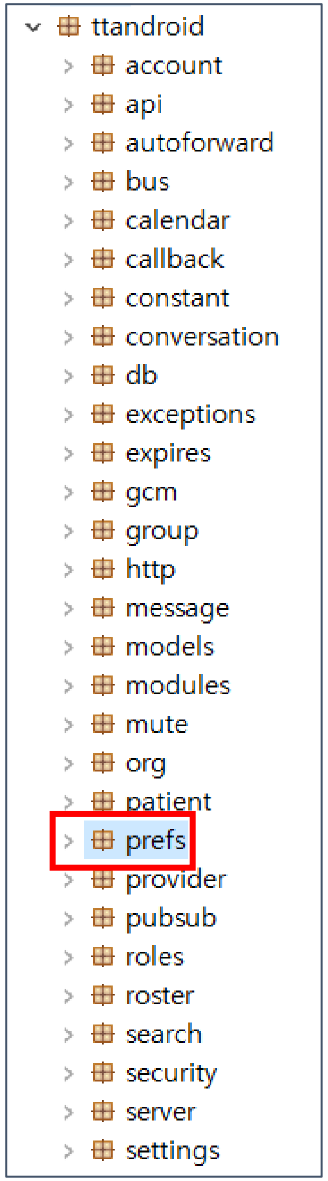
```
C:₩Users₩kimsu₩OneDrive₩Desktop₩tigerconnect.apk.jdb2
  tigerconnect.apk
    tigerconnect.apk
      Manifest
      Certificate
      Bytecode (Virtual, Merged)
      Resources
```

```
android
androidx
  core
    graphics
  media
    AudioAttributesCompatParcelizer
    AudioAttributesImplApi21Parcelizer
    AudioAttributesImplBaseParcelizer
  versionedparcelable
    CustomVersionedParcelable
    NonParcelField
    ParcelField
    ParcelImpl
    ParcelUtils
    R
    VersionedParcel
    VersionedParcelable
    VersionedParcelize
    a
    b
    c
    d
bolts
  AggregateException
  CancellationToken
```

```
Decompiling at Lbolts/a;
Unit "a" (java) was created
Decompiling at Lcom/tigertext/analytics/AnalyticsConstants;
Unit "AnalyticsConstants" (java) was created
Decompiling at Lcom/tigertext/voip/VoIPManager;->e()Ljava/text/SimpleDateFormat;
Unit "VoIPManager" (java) was created
```

coord: (73669,0,0) | addr: Lcom/tigertext/analytics/AnalyticsConstants; | loc: ?

JEB로 tigerconnect.apk 분석

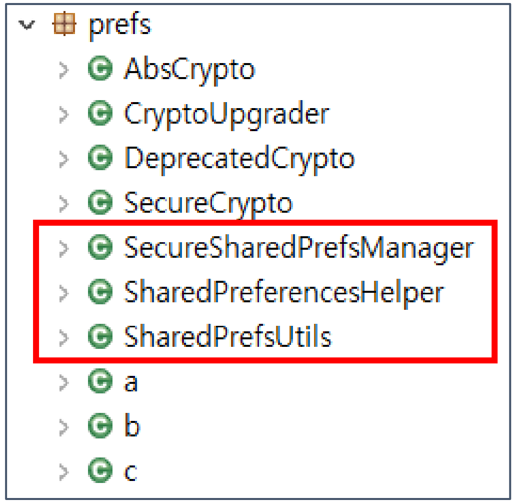


```
ttandroid
  account
  api
  autoforward
  bus
  calendar
  callback
  constant
  conversation
  db
  exceptions
  expires
  gcm
  group
  http
  message
  models
  modules
  mute
  org
  patient
  prefs
  provider
  pubsub
  roles
  roster
  search
  security
  server
  settings
```

1) Class파일 중에 ttandroid 더블클릭

2) Prefs 더블클릭

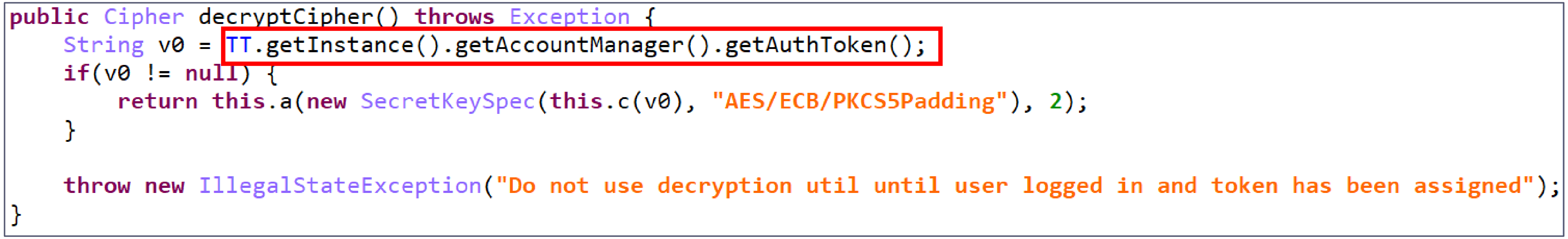
3) Sharedprefs 함수들 살펴보기



```
prefs
  AbsCrypto
  CryptoUpgrader
  DeprecatedCrypto
  SecureCrypto
  SecureSharedPrefsManager
  SharedPreferencesHelper
  SharedPrefsUtils
  a
  b
  c
```

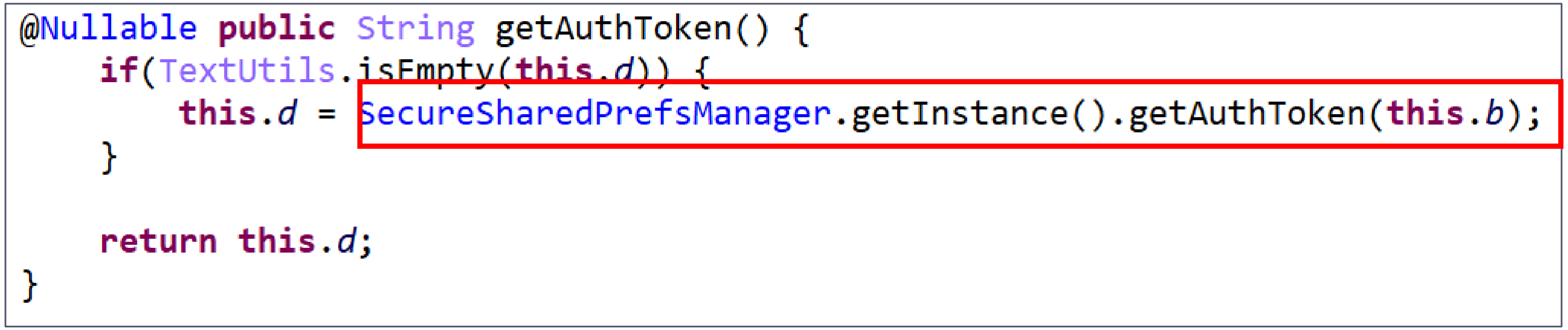
JEB로 tigerconnect.apk 분석

- decryptCipher()



```
public Cipher decryptCipher() throws Exception {
    String v0 = TT.getInstance().getAccountManager().getAuthToken();
    if(v0 != null) {
        return this.a(new SecretKeySpec(this.c(v0), "AES/ECB/PKCS5Padding"), 2);
    }

    throw new IllegalStateException("Do not use decryption util until user logged in and token has been assigned");
}
```

- getAuthToken()

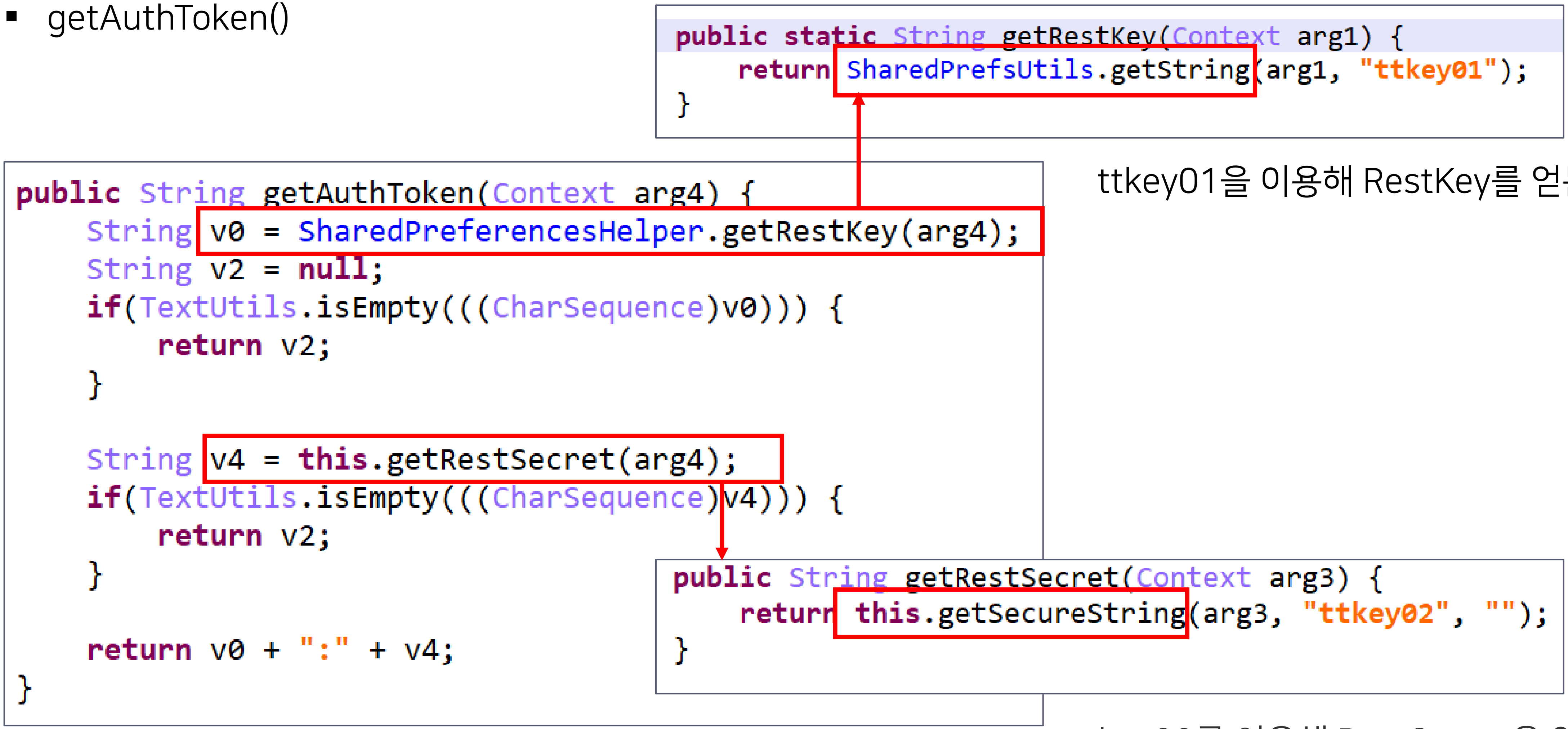


```
@Nullable public String getAuthToken() {
    if(TextUtils.isEmpty(this.d)) {
        this.d = SecureSharedPrefsManager.getInstance().getAuthToken(this.b);
    }

    return this.d;
}
```

SecureSharePrefsManager.getAuthToken 반환

JEB로 tigerconnect.apk 분석

- getAuthToken()



```
public static String getRestKey(Context arg1) {
    return SharedPrefsUtils.getString(arg1, "ttkey01");
}
```

ttkey01을 이용해 RestKey를 얻는다.

```
public String getAuthToken(Context arg4) {
    String v0 = SharedPreferencesHelper.getRestKey(arg4);
    String v2 = null;
    if(TextUtils.isEmpty(((CharSequence)v0))) {
        return v2;
    }

    String v4 = this.getRestSecret(arg4);
    if(TextUtils.isEmpty(((CharSequence)v4))) {
        return v2;
    }

    return v0 + ":" + v4;
}
```

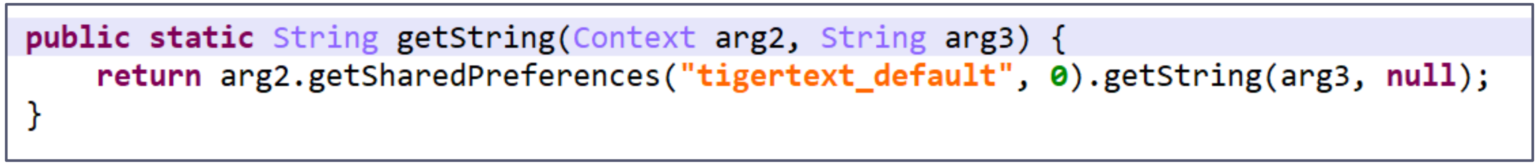
```
public String getRestSecret(Context arg3) {
    return this.getSecureString(arg3, "ttkey02", "");
}
```

ttkey02를 이용해 RestSecret을 얻는다.

[v0 + ":“ + v4] = [RestKey : RestSecret]으로 값을 반환.

JEB로 tigerconnect.apk 분석

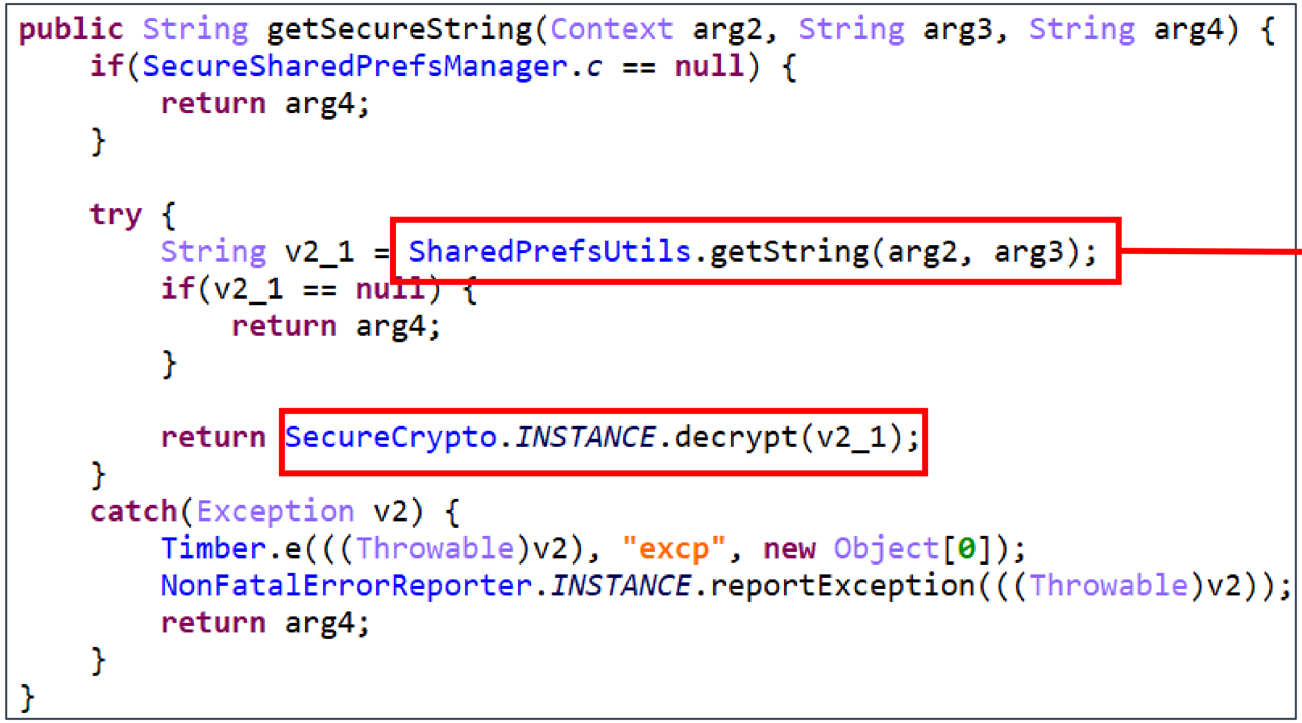
- getString()



```
public static String getString(Context arg2, String arg3) {
    return arg2.getSharedPreferences("tigertext_default", 0).getString(arg3, null);
}
```

ttkey01의 String 얻는 함수

- getSecureString

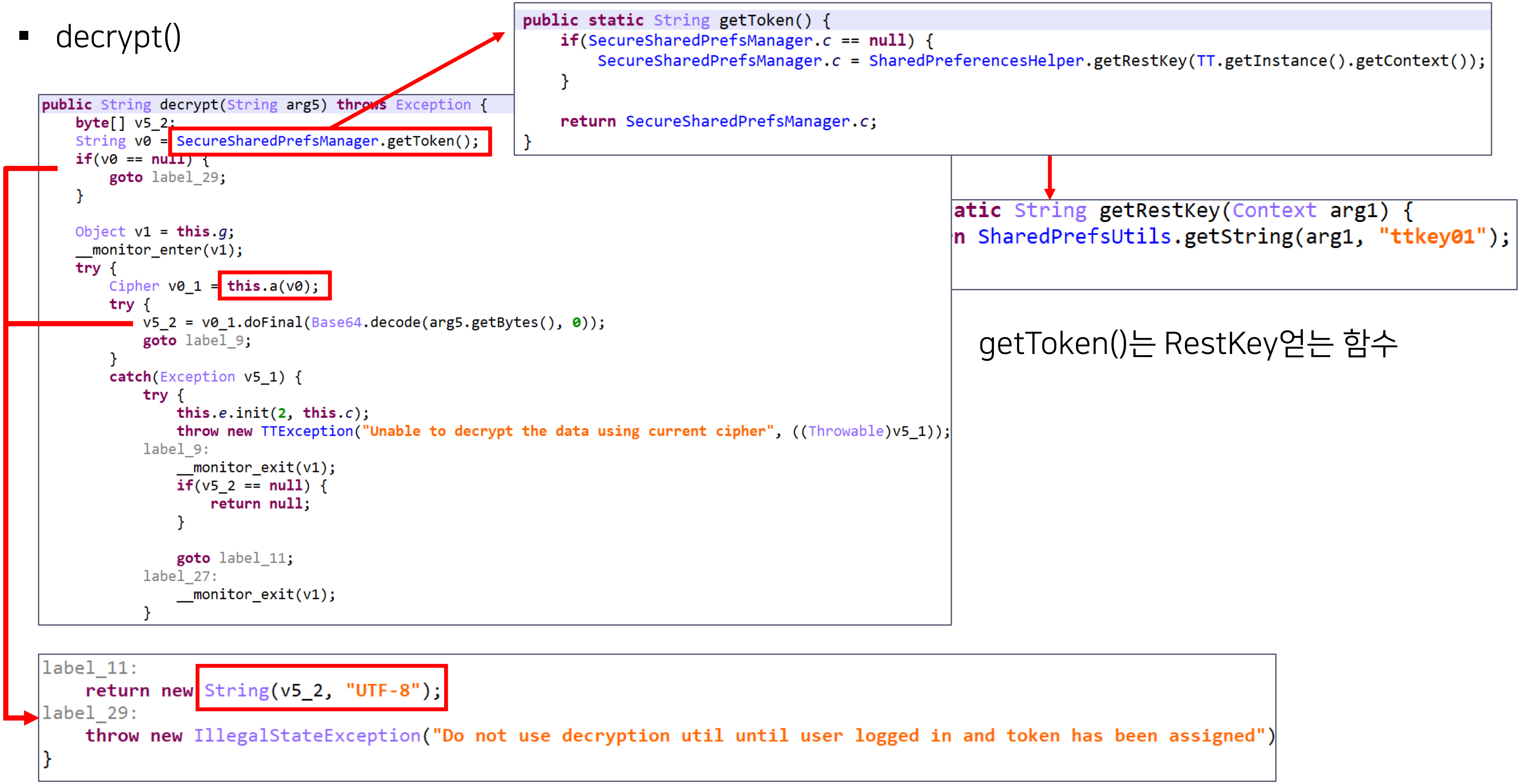


```
public String getSecureString(Context arg2, String arg3, String arg4) {
    if(SecureSharedPrefsManager.c == null) {
        return arg4;
    }

    try {
        String v2_1 = SharedPrefsUtils.getString(arg2, arg3);
        if(v2_1 == null) {
            return arg4;
        }

        return SecureCrypto.INSTANCE.decrypt(v2_1);
    }
    catch(Exception v2) {
        Timber.e(((Throwable)v2), "excp", new Object[0]);
        NonFatalErrorReporter.INSTANCE.reportException(((Throwable)v2));
        return arg4;
    }
}
```

ttkey02의 String 얻는함수

JEB로 tigerconnect.apk 분석

- decrypt()



```
public static String getToken() {
    if(SecureSharedPrefsManager.c == null) {
        SecureSharedPrefsManager.c = SharedPreferencesHelper.getRestKey(TT.getInstance().getContext());
    }

    return SecureSharedPrefsManager.c;
}
```

```
atic String getRestKey(Context arg1) {
n SharedPrefsUtils.getString(arg1, "ttkey01");
```

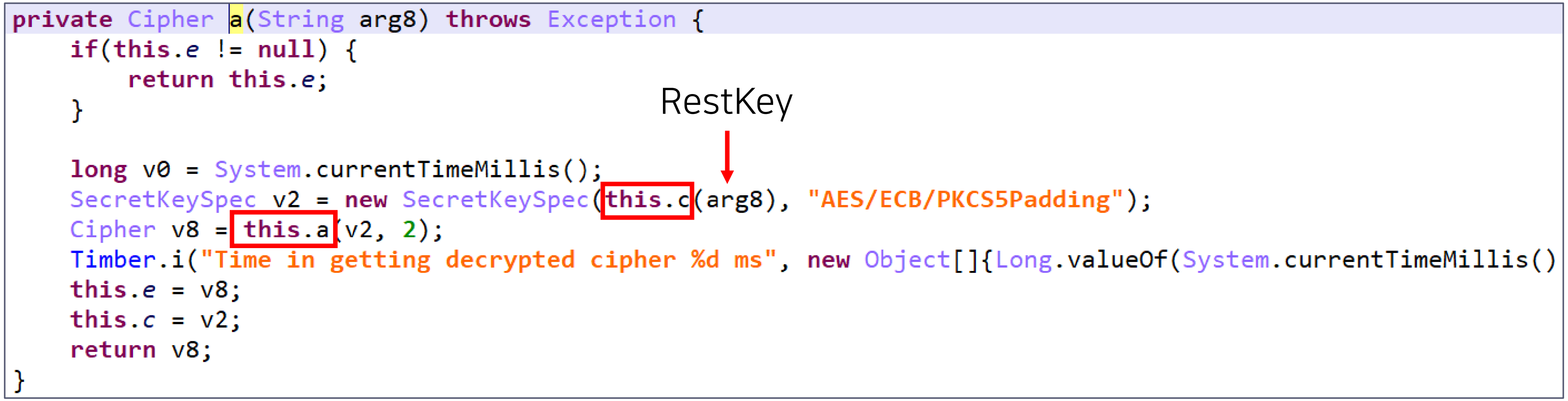
getToken()는 RestKey얻는 함수

```
public String decrypt(String arg5) throws Exception {
    byte[] v5_2;
    String v0 = SecureSharedPrefsManager.getToken();
    if(v0 == null) {
        goto label_29;
    }

    Object v1 = this.g;
    __monitor_enter(v1);
    try {
        Cipher v0_1 = this.a(v0);
        try {
            v5_2 = v0_1.doFinal(Base64.decode(arg5.getBytes(), 0));
            goto label_9;
        }
        catch(Exception v5_1) {
            try {
                this.e.init(2, this.c);
                throw new TTException("Unable to decrypt the data using current cipher", ((Throwable)v5_1));
            label_9:
                __monitor_exit(v1);
                if(v5_2 == null) {
                    return null;
                }

                goto label_11;
            label_27:
                __monitor_exit(v1);
            }
```

```
label_11:
    return new String(v5_2, "UTF-8");
label_29:
    throw new IllegalStateException("Do not use decryption util until user logged in and token has been assigned")
}
```

JEB로 tigerconnect.apk 분석

- a()

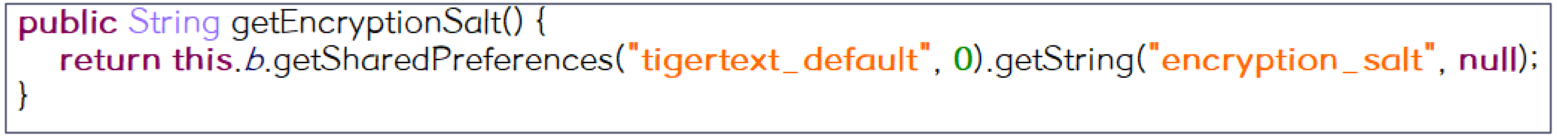


```java
private Cipher a(String arg8) throws Exception {
    if(this.e != null) {
        return this.e;
    }

    long v0 = System.currentTimeMillis();
    SecretKeySpec v2 = new SecretKeySpec(this.c(arg8), "AES/ECB/PKCS5Padding");
    Cipher v8 = this.a(v2, 2);
    Timber.i("Time in getting decrypted cipher %d ms", new Object[]{Long.valueOf(System.currentTimeMillis()
    this.e = v8;
    this.c = v2;
    return v8;
}
```

RestKey

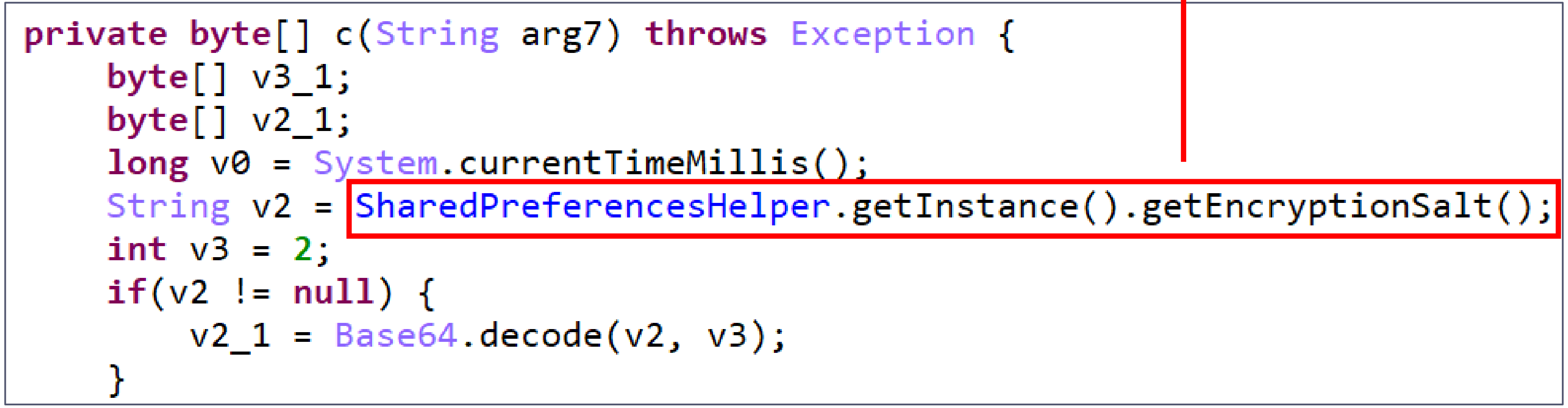
JEB로 tigerconnect.apk 분석

- c()



```
public String getEncryptionSalt() {
    return this.b.getSharedPreferences("tigertext_default", 0).getString("encryption_salt", null);
}
```

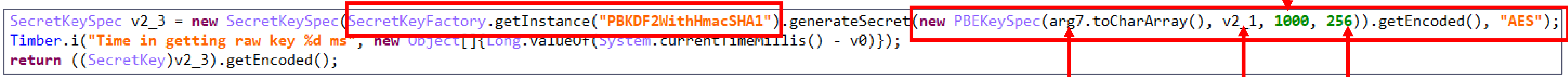
Salt값 얻기



```
private byte[] c(String arg7) throws Exception {
    byte[] v3_1;
    byte[] v2_1;
    long v0 = System.currentTimeMillis();
    String v2 = SharedPreferencesHelper.getInstance().getEncryptionSalt();
    int v3 = 2;
    if(v2 != null) {
        v2_1 = Base64.decode(v2, v3);
    }
```

iteration

PBKDF2-SHA1 이용해서 Secretkey 생성



```
SecretKeySpec v2_3 = new SecretKeySpec(SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1").generateSecret(new PBEKeySpec(arg7.toCharArray(), v2_1, 1000, 256)).getEncoded(), "AES");
Timber.i("Time in getting raw key %d ms", new Object[]{Long.valueOf(System.currentTimeMillis() - v0)});
return ((SecretKey)v2_3).getEncoded();
```

Secretkey 반환

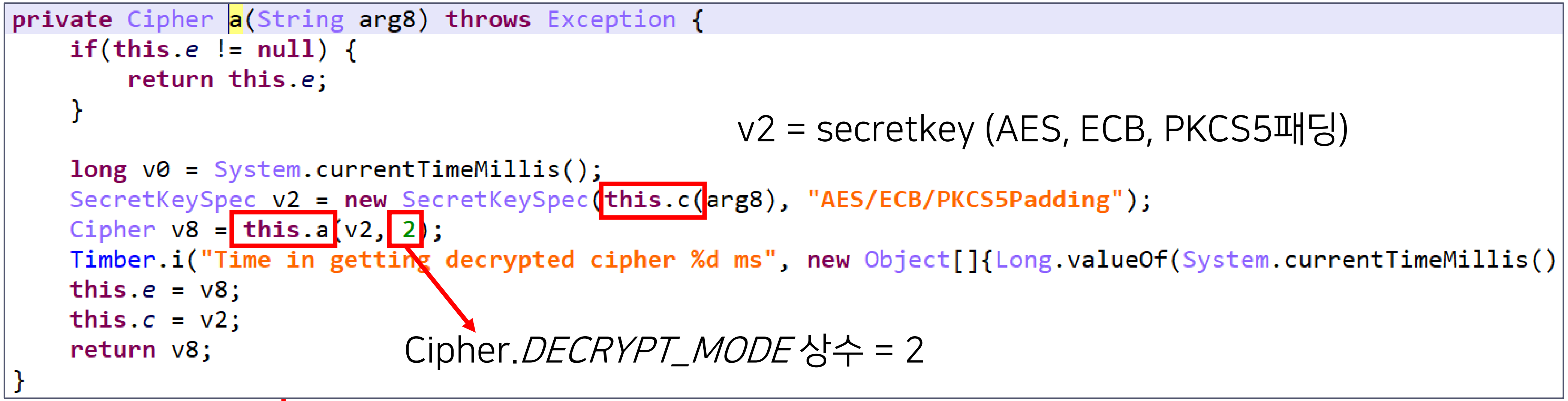
restKey

salt

Key len

JEB로 tigerconnect.apk 분석

- a()

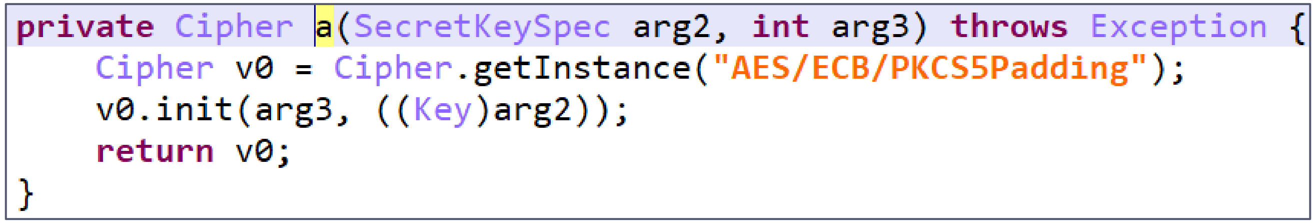


```
private Cipher a(String arg8) throws Exception {
    if(this.e != null) {
        return this.e;
    }

    long v0 = System.currentTimeMillis();
    SecretKeySpec v2 = new SecretKeySpec(this.c(arg8), "AES/ECB/PKCS5Padding");
    Cipher v8 = this.a(v2, 2);
    Timber.i("Time in getting decrypted cipher %d ms", new Object[]{Long.valueOf(System.currentTimeMillis()
    this.e = v8;
    this.c = v2;
    return v8;
}
```

v2 = secretkey (AES, ECB, PKCS5패딩)

Cipher.*DECRYPT_MODE* 상수 = 2

- a()

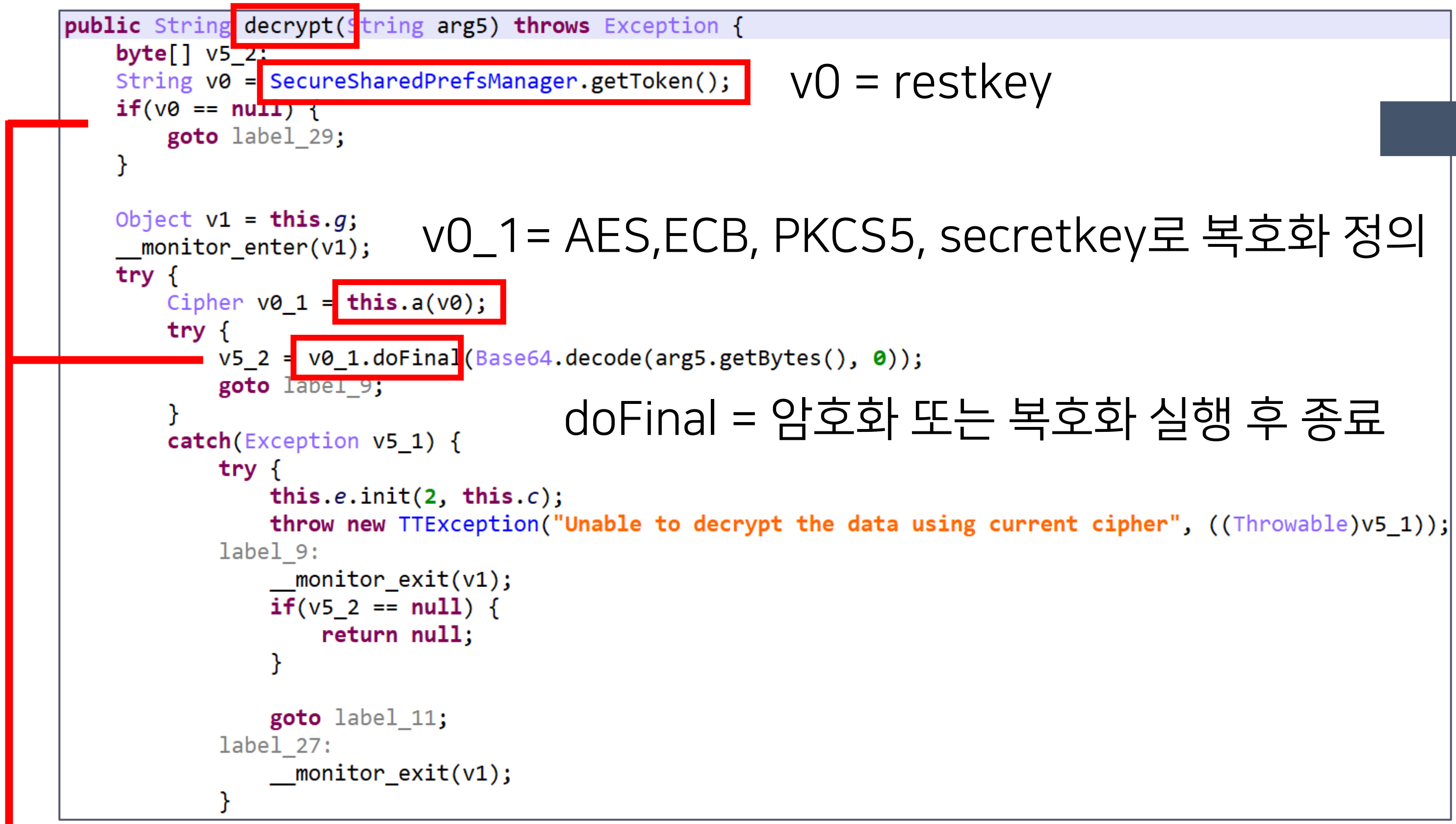


```
private Cipher a(SecretKeySpec arg2, int arg3) throws Exception {
    Cipher v0 = Cipher.getInstance("AES/ECB/PKCS5Padding");
    v0.init(arg3, ((Key)arg2));
    return v0;
}
```

➡ AES, ECB, PKCS5패딩, KEY=secretkey로 복호화를 정의하는 함수

JEB로 tigerconnect.apk 분석

- decrypt()

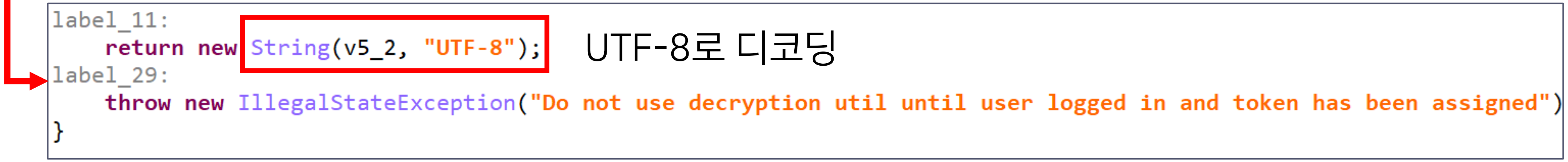


```
public String decrypt(String arg5) throws Exception {
    byte[] v5_2;
    String v0 = SecureSharedPrefsManager.getToken();
    if(v0 == null) {
        goto label_29;
    }

    Object v1 = this.g;
    __monitor_enter(v1);
    try {
        Cipher v0_1 = this.a(v0);
        try {
            v5_2 = v0_1.doFinal(Base64.decode(arg5.getBytes(), 0));
            goto label_9;
        }
        catch(Exception v5_1) {
            try {
                this.e.init(2, this.c);
                throw new TTException("Unable to decrypt the data using current cipher", ((Throwable)v5_1));
            label_9:
                __monitor_exit(v1);
                if(v5_2 == null) {
                    return null;
                }

                goto label_11;
            label_27:
                __monitor_exit(v1);
            }
```

v0 = restkey

v0_1= AES,ECB, PKCS5, secretkey로 복호화 정의

doFinal = 암호화 또는 복호화 실행 후 종료



```
label_11:
    return new String(v5_2, "UTF-8");
label_29:
    throw new IllegalStateException("Do not use decryption util until user logged in and token has been assigned")
}
```

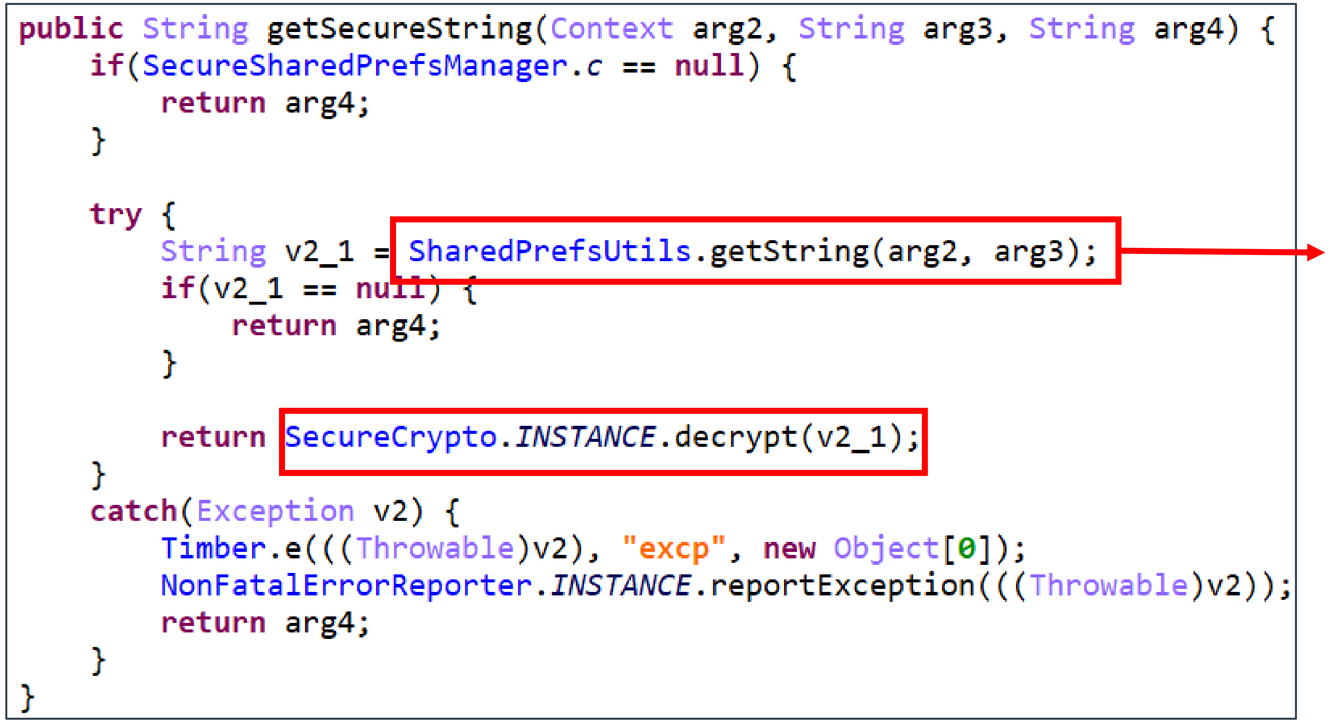
UTF-8로 디코딩

- decrypt(ttkey02) –

1. ttkey02로 restkey 생성
2. restkey로 pbkdf-sha1 이용해서 secretkey 생성
3. 복호화
   → AES, ECB, PKCS5, 비밀키
4. UTF-8로 디코딩해서 출력

JEB로 tigerconnect.apk 분석

- getSecureString



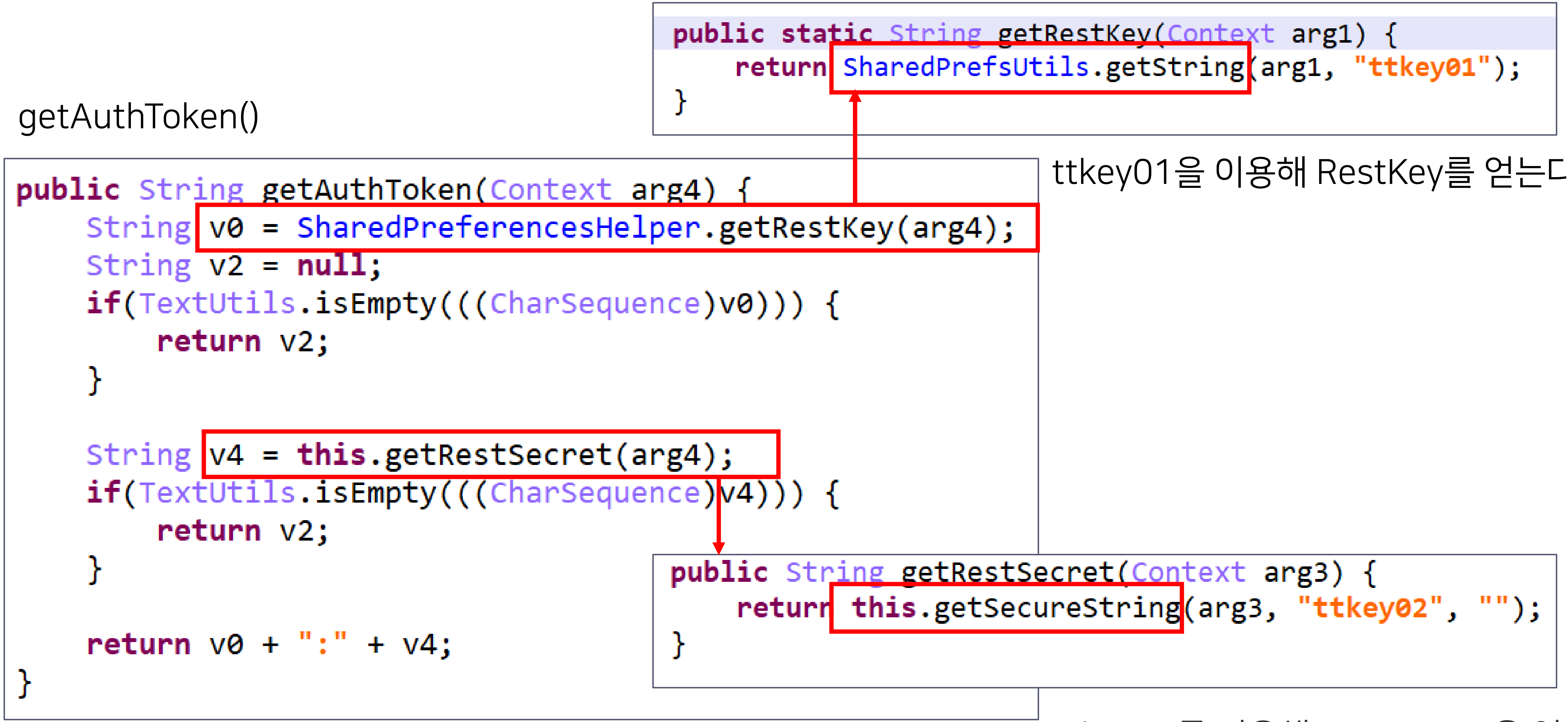
```
public String getSecureString(Context arg2, String arg3, String arg4) {
    if(SecureSharedPrefsManager.c == null) {
        return arg4;
    }

    try {
        String v2_1 = SharedPrefsUtils.getString(arg2, arg3);
        if(v2_1 == null) {
            return arg4;
        }

        return SecureCrypto.INSTANCE.decrypt(v2_1);
    }
    catch(Exception v2) {
        Timber.e(((Throwable)v2), "excp", new Object[0]);
        NonFatalErrorReporter.INSTANCE.reportException(((Throwable)v2));
        return arg4;
    }
}
```

ttkey02의 String 얻는함수

ttkey02의 String을 decrypt해서
restsecret을 얻는다.

JEB로 tigerconnect.apk 분석

- getAuthToken()



```
public static String getRestKey(Context arg1) {
    return SharedPrefsUtils.getString(arg1, "ttkey01");
}
```

```
public String getAuthToken(Context arg4) {
    String v0 = SharedPreferencesHelper.getRestKey(arg4);
    String v2 = null;
    if(TextUtils.isEmpty(((CharSequence)v0))) {
        return v2;
    }

    String v4 = this.getRestSecret(arg4);
    if(TextUtils.isEmpty(((CharSequence)v4))) {
        return v2;
    }

    return v0 + ":" + v4;
}
```

```
public String getRestSecret(Context arg3) {
    return this.getSecureString(arg3, "ttkey02", "");
}
```

ttkey01을 이용해 RestKey를 얻는다.

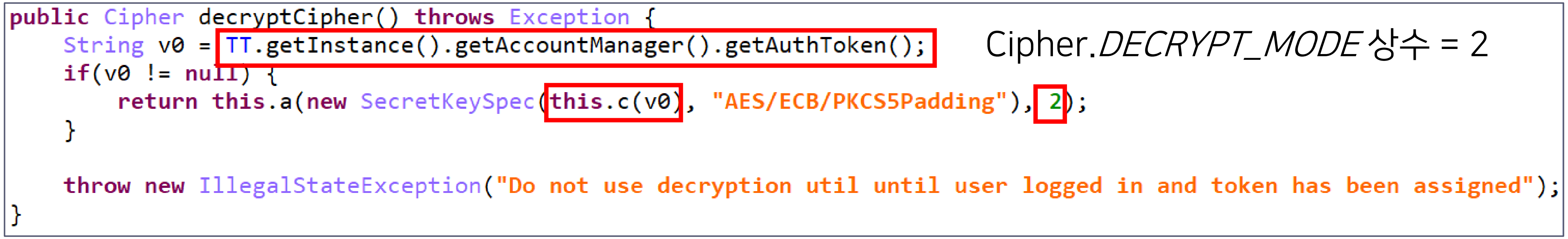
ttkey02를 이용해 RestSecret을 얻는다.

➡ Authtoken = [v0 + ":" + v4] = [RestKey : RestSecret]

JEB로 tigerconnect.apk 분석

- decryptCipher()

V0 = authtoken = [RestKey : RestSecret]

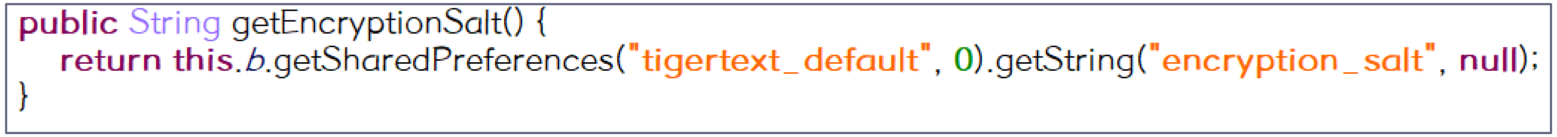


```
public Cipher decryptCipher() throws Exception {
    String v0 = TT.getInstance().getAccountManager().getAuthToken();
    if(v0 != null) {
        return this.a(new SecretKeySpec(this.c(v0), "AES/ECB/PKCS5Padding"), 2);
    }

    throw new IllegalStateException("Do not use decryption util until user logged in and token has been assigned");
}
```

Cipher.*DECRYPT_MODE* 상수 = 2

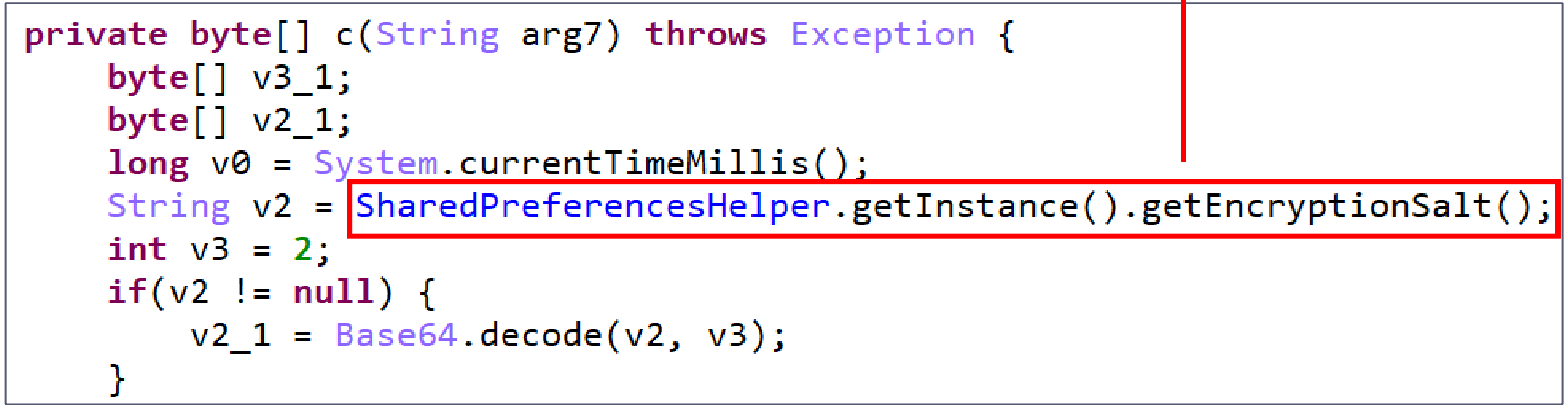
JEB로 tigerconnect.apk 분석

- c()



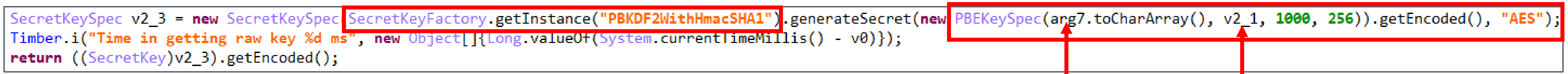
```
public String getEncryptionSalt() {
    return this.b.getSharedPreferences("tigertext_default", 0).getString("encryption_salt", null);
}
```

Salt값 얻기



```
private byte[] c(String arg7) throws Exception {
    byte[] v3_1;
    byte[] v2_1;
    long v0 = System.currentTimeMillis();
    String v2 = SharedPreferencesHelper.getInstance().getEncryptionSalt();
    int v3 = 2;
    if(v2 != null) {
        v2_1 = Base64.decode(v2, v3);
    }
```

PBKDF2-SHA1 이용해서 Secretkey2 생성



```
SecretKeySpec v2_3 = new SecretKeySpec(SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1").generateSecret(new PBEKeySpec(arg7.toCharArray(), v2_1, 1000, 256)).getEncoded(), "AES");
Timber.i("Time in getting raw key %d ms", new Object[]{Long.valueOf(System.currentTimeMillis() - v0)});
return ((SecretKey)v2_3).getEncoded();
```

authtoken

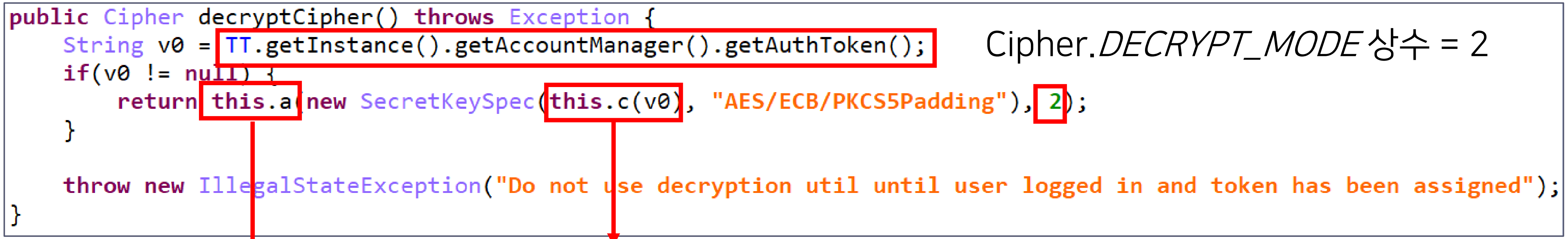
salt

Secretkey2 v2_3 반환

JEB로 tigerconnect.apk 분석

- decryptCipher()

V0 = authtoken = [RestKey : RestSecret]

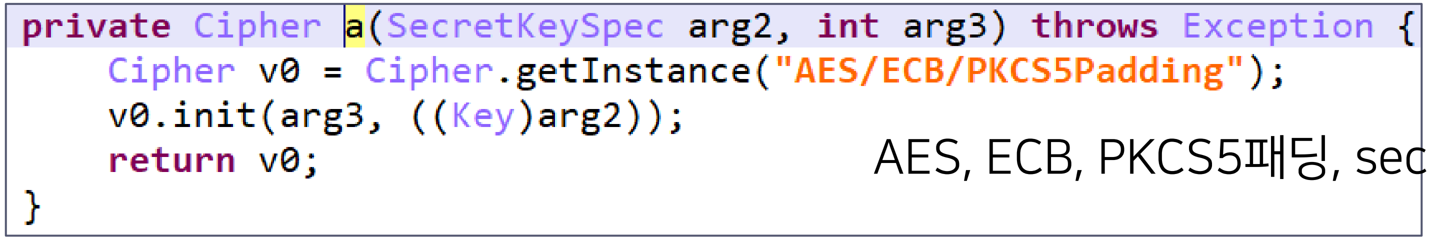


```
public Cipher decryptCipher() throws Exception {
    String v0 = TT.getInstance().getAccountManager().getAuthToken();
    if(v0 != null) {
        return this.a(new SecretKeySpec(this.c(v0), "AES/ECB/PKCS5Padding"), 2);
    }

    throw new IllegalStateException("Do not use decryption util until user logged in and token has been assigned");
}
```

Cipher.*DECRYPT_MODE* 상수 = 2

“secretkey2” 생성

- a()



```
private Cipher a(SecretKeySpec arg2, int arg3) throws Exception {
    Cipher v0 = Cipher.getInstance("AES/ECB/PKCS5Padding");
    v0.init(arg3, ((Key)arg2));
    return v0;
}
```

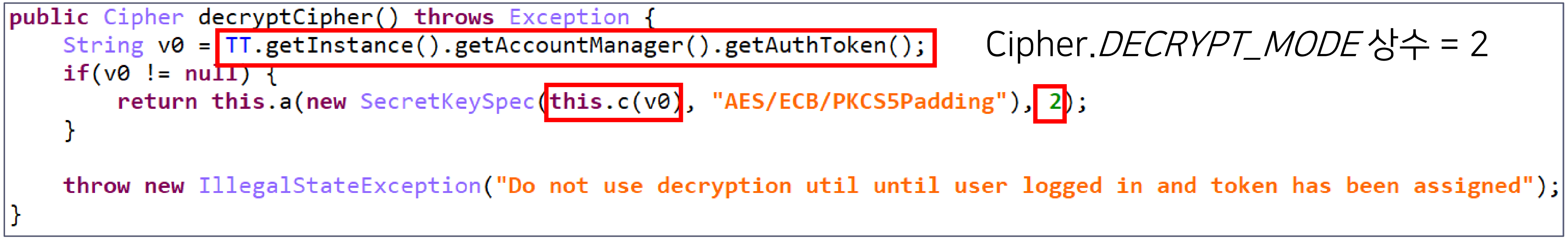
AES, ECB, PKCS5패딩, secretkey2로 복호화를 정의하는 함수

decryptCipher()은 AES, ECB, PKCS5패딩, secretkey2를 사용하는 복호화 함수.

JEB로 tigerconnect.apk 분석

- decryptCipher()

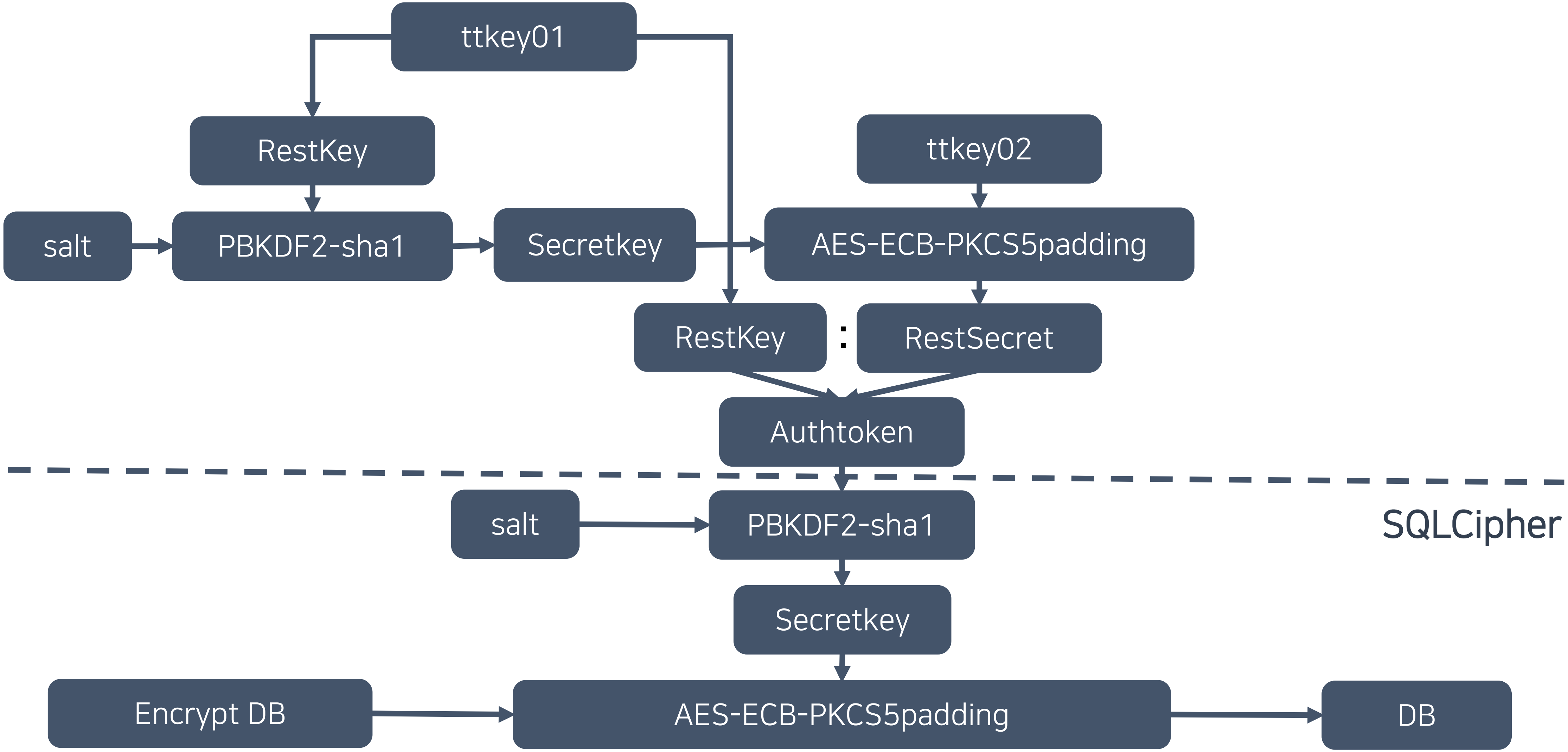
V0 = authtoken = [RestKey : RestSecret]



```
public Cipher decryptCipher() throws Exception {
    String v0 = TT.getInstance().getAccountManager().getAuthToken();
    if(v0 != null) {
        return this.a(new SecretKeySpec(this.c(v0), "AES/ECB/PKCS5Padding"), 2);
    }

    throw new IllegalStateException("Do not use decryption util until user logged in and token has been assigned");
}
```

Cipher.*DECRYPT_MODE* 상수 = 2

JEB로 tigerconnect.apk 분석


ttkey01
RestKey
ttkey02
salt
PBKDF2-sha1
Secretkey
AES-ECB-PKCS5padding
RestKey
:
RestSecret
Authtoken
salt
PBKDF2-sha1
SQLCipher
Secretkey
Encrypt DB
AES-ECB-PKCS5padding
DB