http://resources.infosecinstitute.com/android-hacking-security-part-16-broken-cryptography/
Часть 16. Пример слабой криптографии в apk.

Шифрование. Применение слабых компонентов системы (ключей, алгоритмов), либо их комбинаций.
Кодирование — не шифрование.

Пример 1. Слабый хеш: MD5. Давно устарел и с высокой вероятностью можно получить материал дающий такое же значение.
Пример 2. base64. Кодирование — не шифрование. Нет секретного компонента.
Пример 3. Кривые руки: секрет фиксирован и вшит в АПК. На примере использования SQLCipher.
Либа: https://www.zetetic.net/sqlcipher/open-source/
Утилиты:
https://code.google.com/p/dex2jar/

Забираем криптованную БД с устройства
adb pull /data/data/[packagename]/databases/filename.db
Проверяем что штатная утиль SQLite3 не читает БД
> sqlite2 filename.db
>.tables
Ошибка: файл шифрован или блаблабла.

Разбираем АПК на части
unzip SecureSQLite.apk

Файл classes.dex конвертим в jar для анализа
dex2jar classes.dex –o classes.jar

Берем любой java-декомпиль (например, JD-GUI) и смотрим java-код.
…
import net.sqlcipher.database.SQLiteDatabase;
…
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(file, “password”, null);
…

Берем утилиту SQLCipher с http://sqlcipher.net/open-source/ , а дальше дело техники.
>sqlcipher filename.db
>PRAGMA key = 'password'
>.tables
…