File encryption

You work for a mobile device manufacturer and you have been asked to chose a type of device encryption for your next Android smartphone. You can chose between full-disk encryption (FDE) and file based encryption (FBE). Now, consider the following scenarios

A. Market research has shown that users are interested in "transparent operation mode“
   1. What does "transparent operation mode" mean?
   2. What are the security guarantees that you can offer to users which activate the "transparent operation mode"?
   3. Which of the two systems (FDE and FBE) is better if you want "transparent operation mode"? Explain your answer.

B. You want to speed up the boot process of your device by encrypting less data.
   1. Which of the two systems (FDE and FBE) will you chose and why?
   2. Give one additional positive feature gained from you choice.
   3. Give a potential negative effect gained from your choice.

File encryption

A. Market research has shown that users are interested in "transparent operation mode“

   1. What does "transparent operation mode" mean?

File encryption

A. Market research has shown that users are interested in "transparent operation mode“
    1. What does "transparent operation mode" mean?

“Transparent operation mode” is a FDE mode where which uses the TPM and where disk decryption happens without any input from the user. In order to protect the encryption keys they are stored inside the a trusted hardware environment and are released only if specific conditions are met (platform has not changed, etc.).

File encryption

A. Market research has shown that users are interested in "transparent operation mode“
    2. What are the security guarantees that you can offer to users which activate the "transparent operation mode"?

File encryption

A. Market research has shown that users are interested in "transparent operation mode“

    2. What are the security guarantees that you can offer to users which activate the "transparent operation mode"?

Drives encrypted in “transparent operation mode” are only decrypted if the TPM can provide attestation of the boot process. As such, users can be assured that their data will only be accessible on the device which performed the encryption if the device has not been tampered with.

File encryption

A. Market research has shown that users are interested in "transparent operation mode“
   1. Which of the two systems (FDE and FBE) is better if you want "transparent operation mode"? Explain your answer.

File encryption

A. Market research has shown that users are interested in "transparent operation mode“
   1. Which of the two systems (FDE and FBE) is better if you want "transparent operation mode"? Explain your answer.

Drives encrypted in “transparent operation mode” usually require FDE. In FDE one key encrypts the whole drive and the key is stored inside trusted hardware module. This key is released during boot only if specific conditions are met.

File encryption

B. You want to speed up the boot process of your device by encrypting less data.

   1. Which of the two systems (FDE and FBE) will you chose and why?

File encryption

B. You want to speed up the boot process of your device by encrypting less data.
    1. Which of the two systems (FDE and FBE) will you chose and why?

FDE: one key encrypts whole drive. This is not the right choice because you cannot tweak the amount of data you encrypt.

FBE: Only parts of the file-system are encrypted. Very tweak-able in terms of the amount of data to be encrypted.

File encryption

B. You want to speed up the boot process of your device by encrypting less data.

   1. Give one additional positive feature gained from you choice.

Advantages:

File encryption

B. You want to speed up the boot process of your device by encrypting less data.

    1. Give one additional positive feature gained from you choice.

Advantages:

- Different keys protect different parts of the file-system. If one key is compromised it does not result in whole system compromise.
- Can be used to encrypt only part of the system
- Can be used to provide cryptographic access control for multiple users.

File encryption

B. You want to speed up the boot process of your device by encrypting less data.

   1. Give one additional negative feature gained from you choice.

Disadvantages:

File encryption

B. You want to speed up the boot process of your device by encrypting less data.

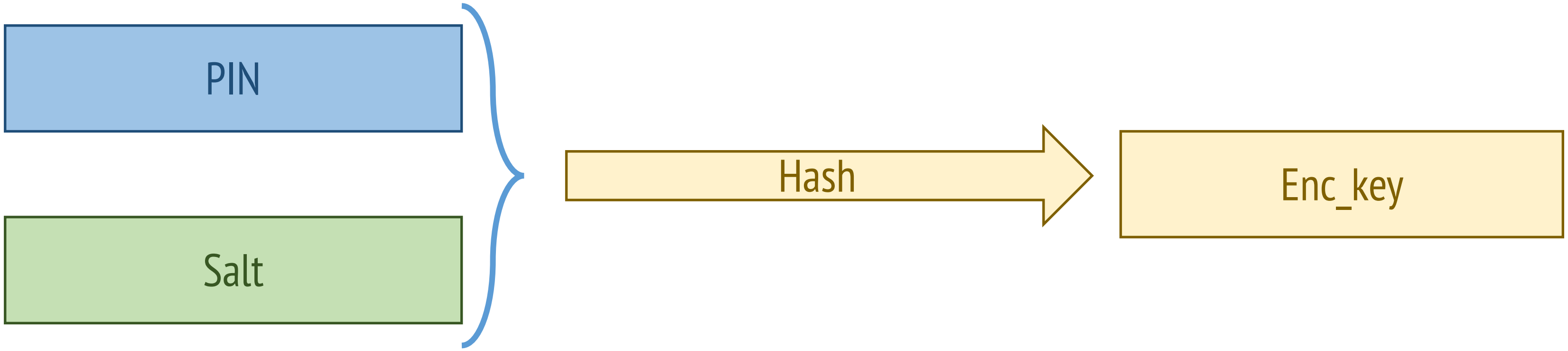
   1. Give one additional negative feature gained from you choice.

Disadvantages:

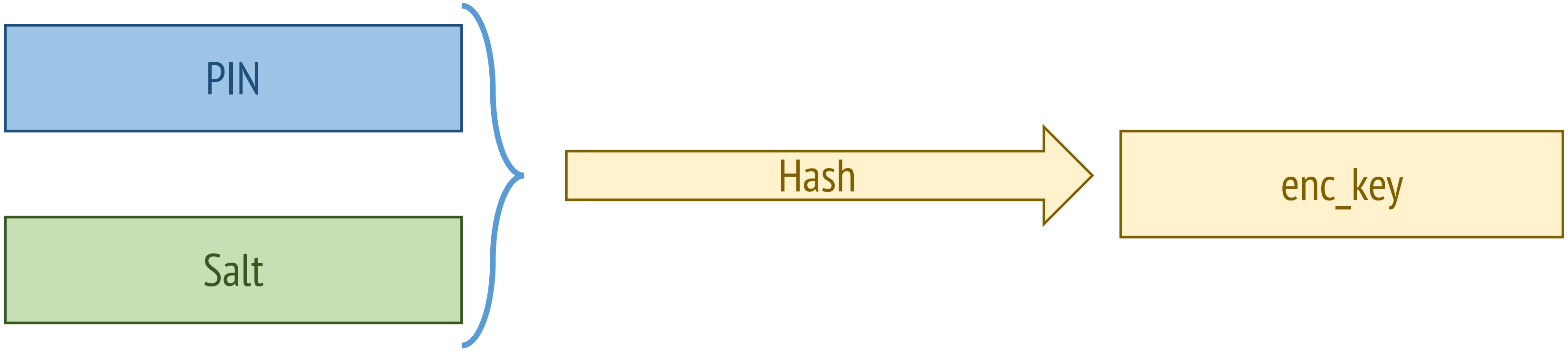
- Does not encrypt disk metadata
- More keys are difficult to manage this can lead to users loosing access to their files, more storage in the trusted hw. module, etc.

File encryption

Consider the key derivation scheme in the figure below, where "PIN" is a 4 digit pin and "salt" is a public random value.

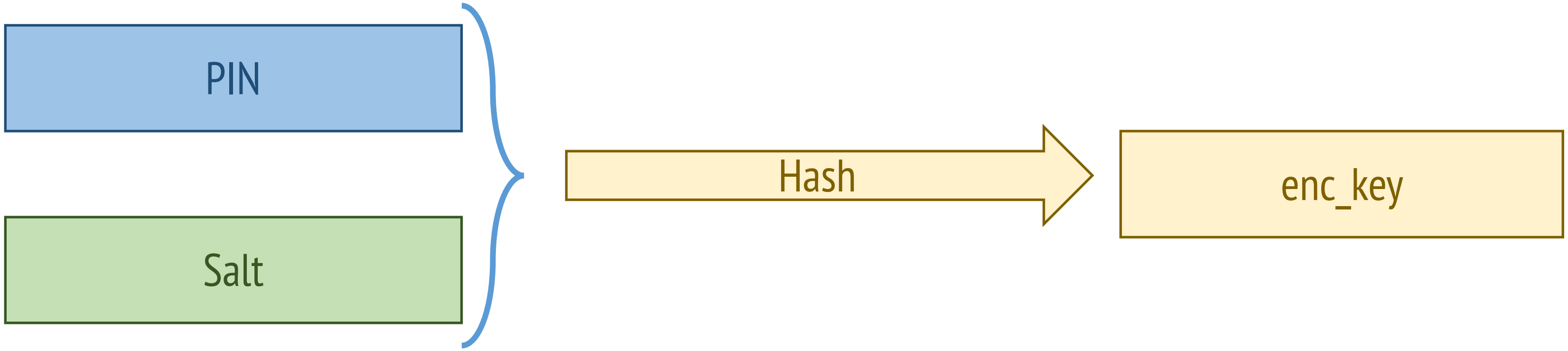


File encryption



Which is the entity being authenticated ?

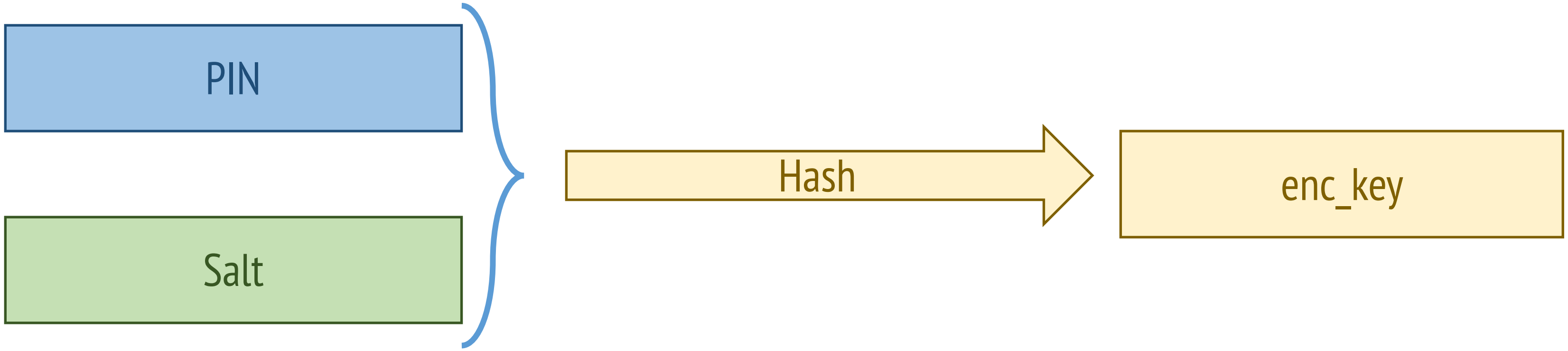
File encryption



Which is the entity being authenticated ?

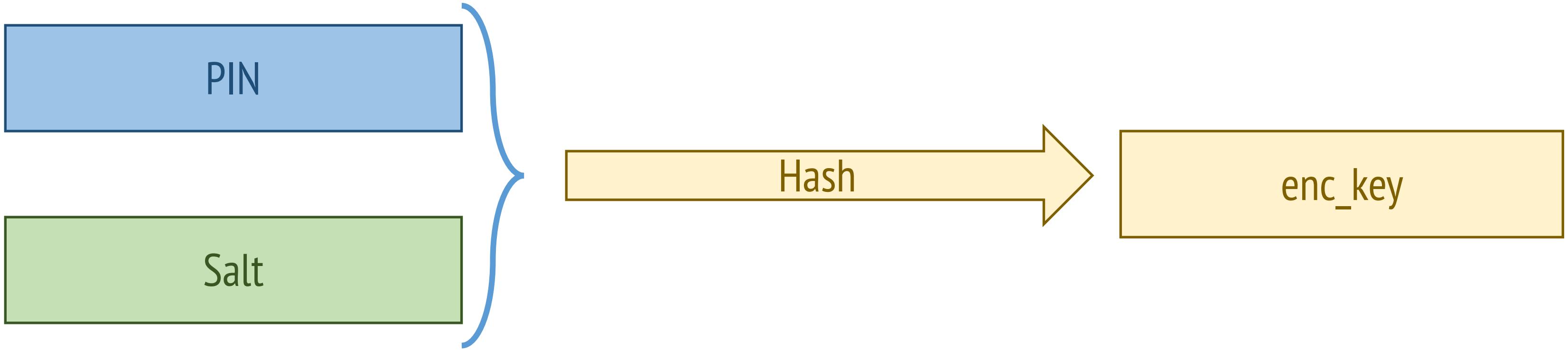
The user through the PIN. There is no contribution from the device. in this scheme.

File encryption



What is the role of the salt?

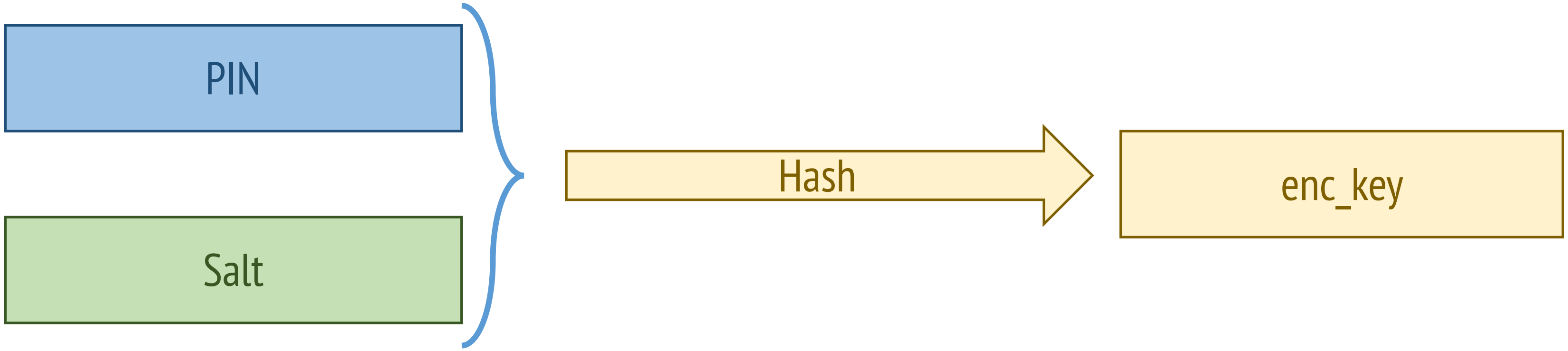
File encryption



What is the role of the salt?

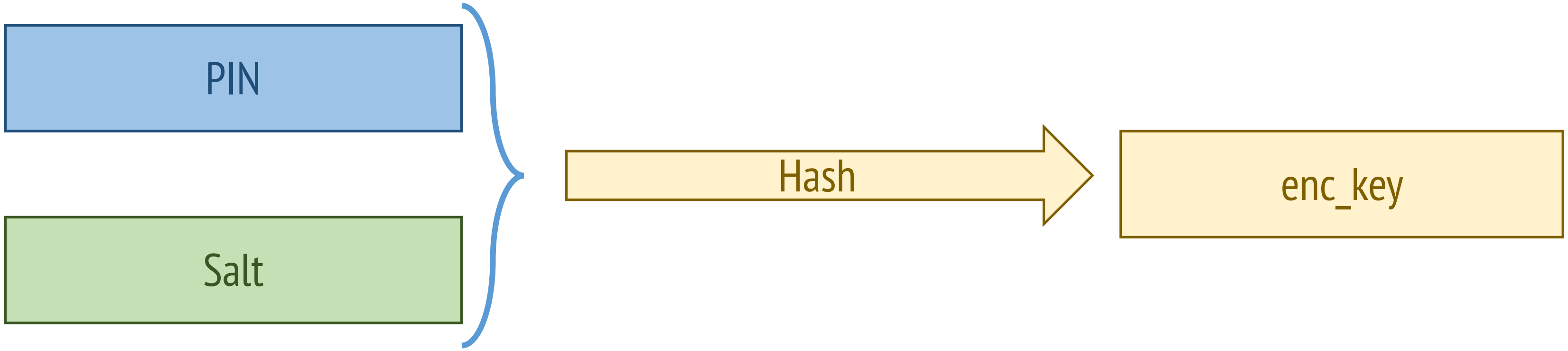
Increase the difficulty of performing dictionary attacks against the PIN.

File encryption



What is the purpose of the hash function?

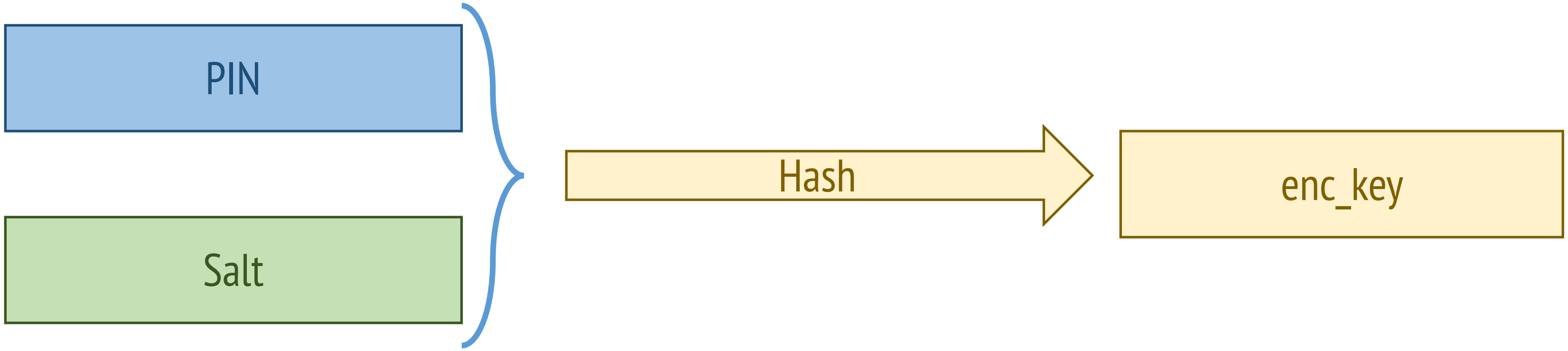
File encryption



What is the purpose of the hash function?

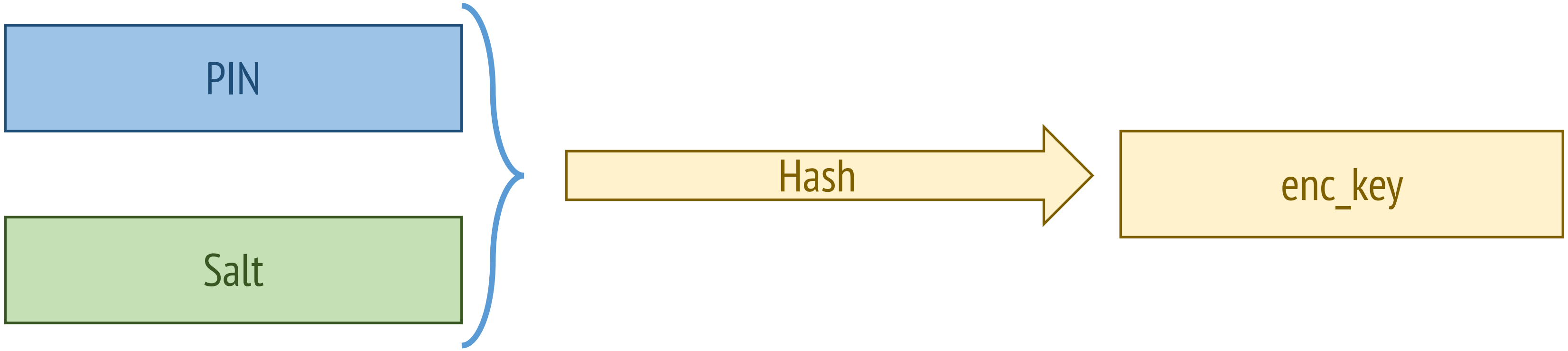
1. Hide the value of the PIN.
2. Provide sufficient entropy for the **enc_key**.

File encryption



Are there any attacks possible against this scheme? Explain your attack and a possible fix for it.

File encryption



Are there any attacks possible against this scheme? Explain your attack and a possible fix for it.

1. The PIN is low entropy. Salt is public. Brute force attacks are easy to mount. **Fix:** include a high entropy secret.
2. The encryption key is not linked to the device. It can be regenerated/captured and reused. **Fix:** Include a secret from the device.
3. Replay attack: capture the *enc_key* and reuse it. **Fix:** include a unique nonce.

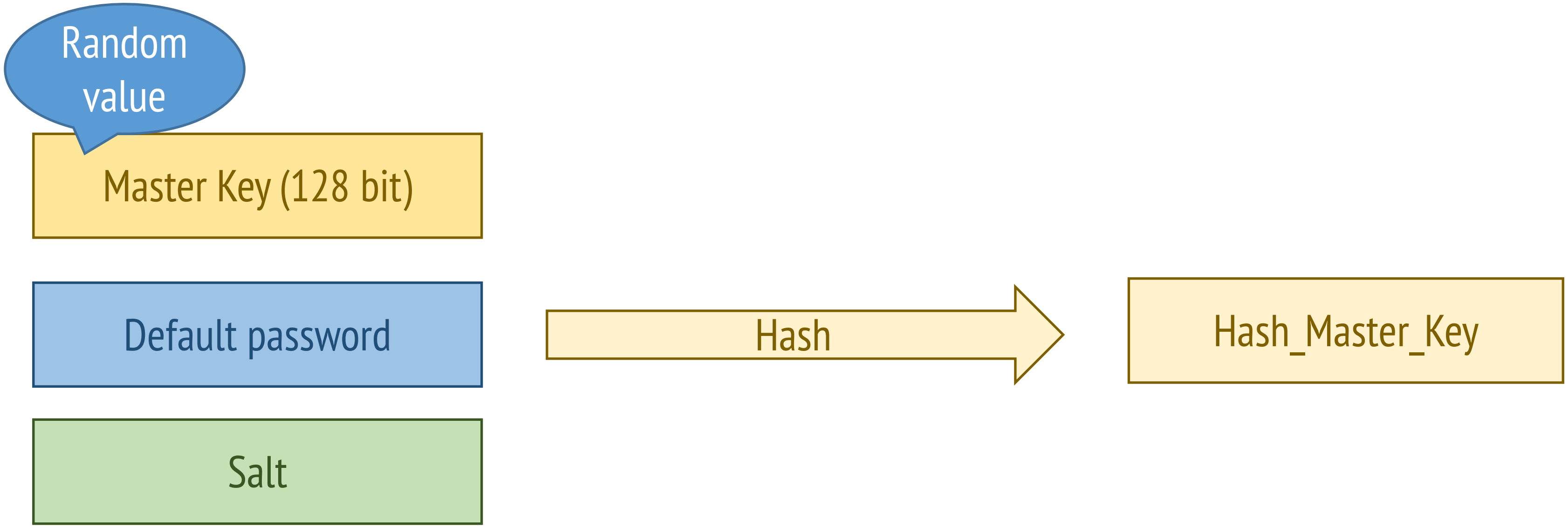
File encryption

What are the security implications of using a public, hardcoded and known value for the “default password” in Android 5.0?

How does it compare to not using encryption at all?

Explain your answers by referring to security aspects (confidentiality, authentication…), and difficulty of use.

Android 5.0 (with Linux kernel & dm-crypt)


Random value
Master Key (128 bit)
Default password
Salt
Hash
Hash_Master_Key