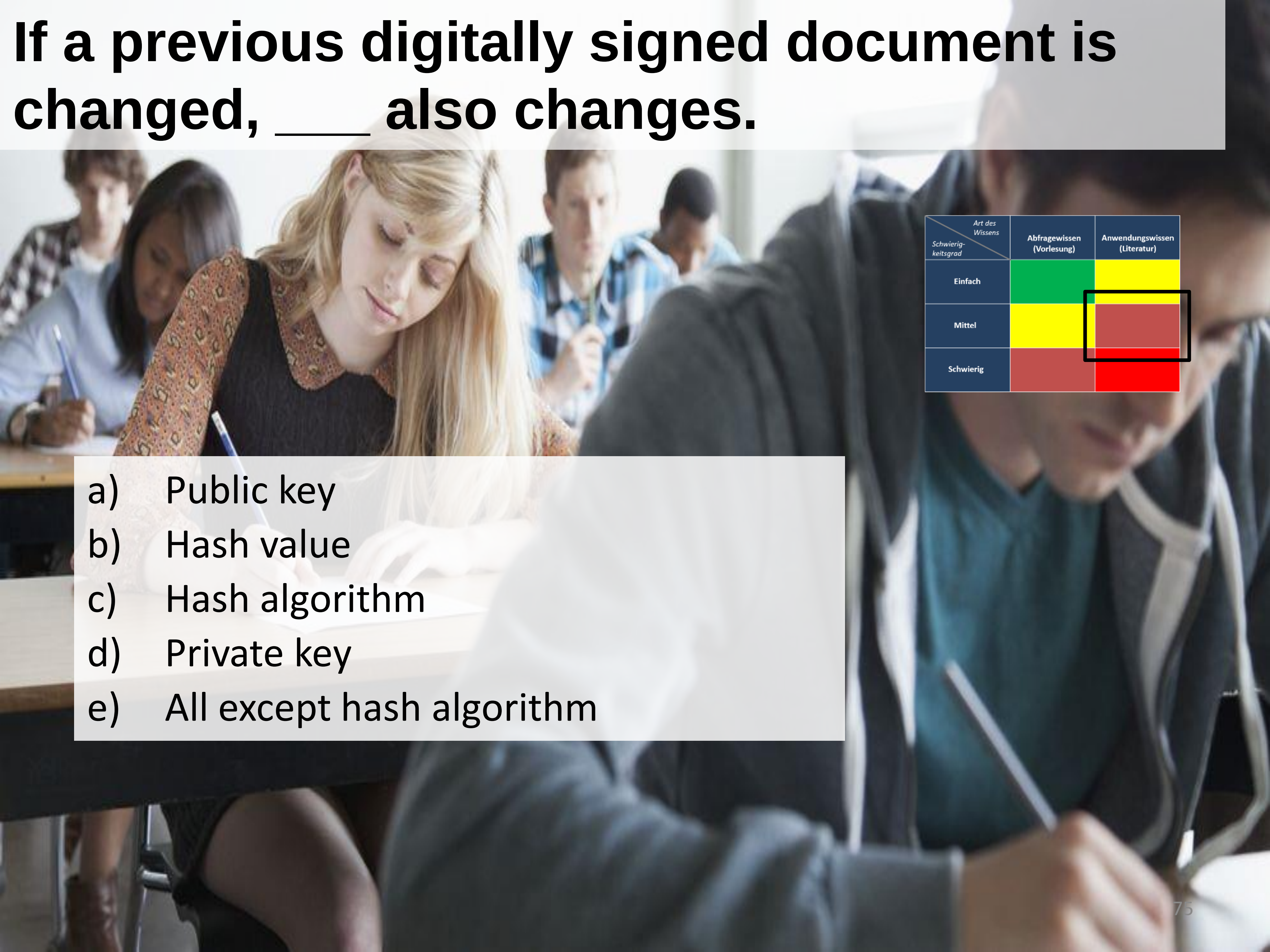
If a previous digitally signed document is changed, ____ also changes.



Art des Wissens Schwierig-keitsgrad	Abfragewissen (Vorlesung)	Anwendungswissen (Literatur)
Einfach	🟩	🟨
Mittel	🟨	🟥
Schwierig	🟥	🟥

a) Public key

b) Hash value

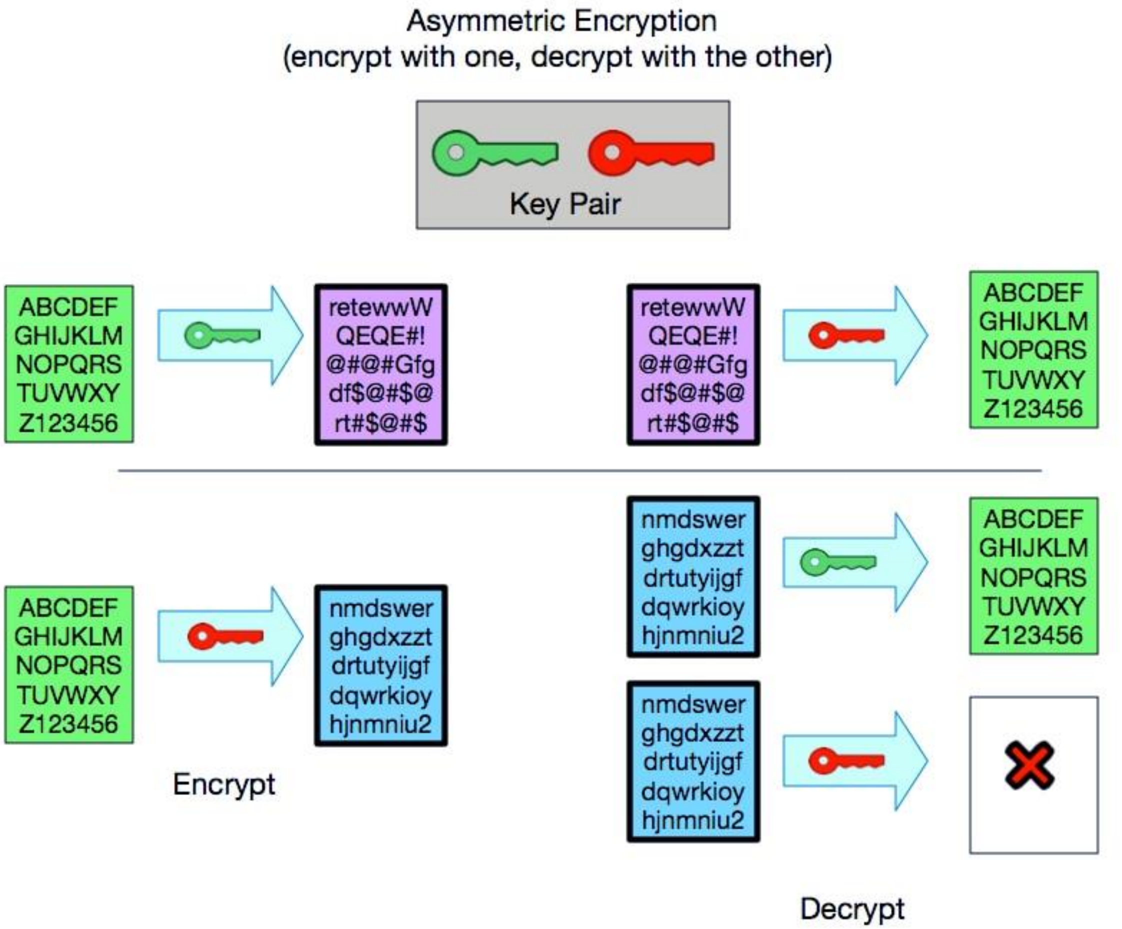
c) Hash algorithm

d) Private key

e) All except hash algorithm

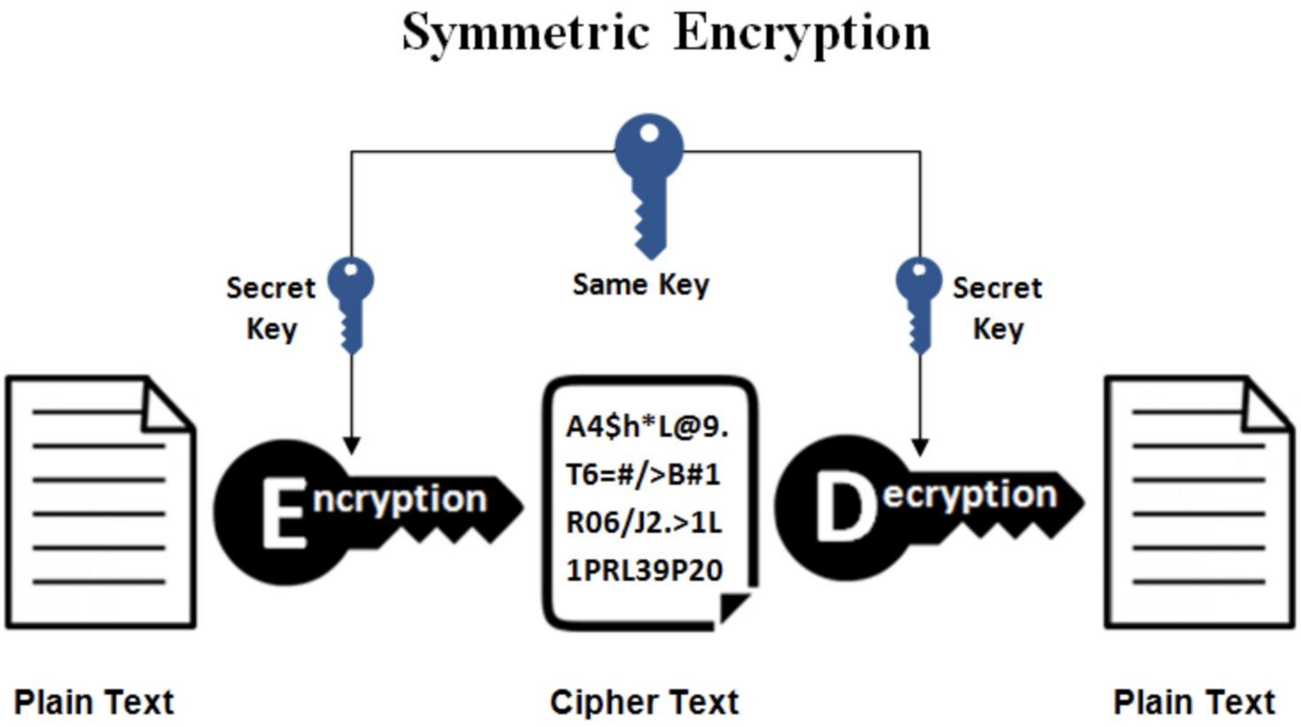
Asymmetrische Verschlüsselung:

Zwei Schlüssel (**Private Key** und **Public Key**)


Asymmetric Encryption
(encrypt with one, decrypt with the other)
Key Pair
ABCDEF GHIJKLM NOPQRS TUVWXY Z123456
retewwW QEQE#! @#@#Gfg df$@#$@ rt#$@#$
retewwW QEQE#! @#@#Gfg df$@#$@ rt#$@#$
ABCDEF GHIJKLM NOPQRS TUVWXY Z123456
ABCDEF GHIJKLM NOPQRS TUVWXY Z123456
nmdswer ghgdxzzt drtutyijgf dqwrkioy hjnmniu2
nmdswer ghgdxzzt drtutyijgf dqwrkioy hjnmniu2
ABCDEF GHIJKLM NOPQRS TUVWXY Z123456
nmdswer ghgdxzzt drtutyijgf dqwrkioy hjnmniu2
Encrypt
Decrypt

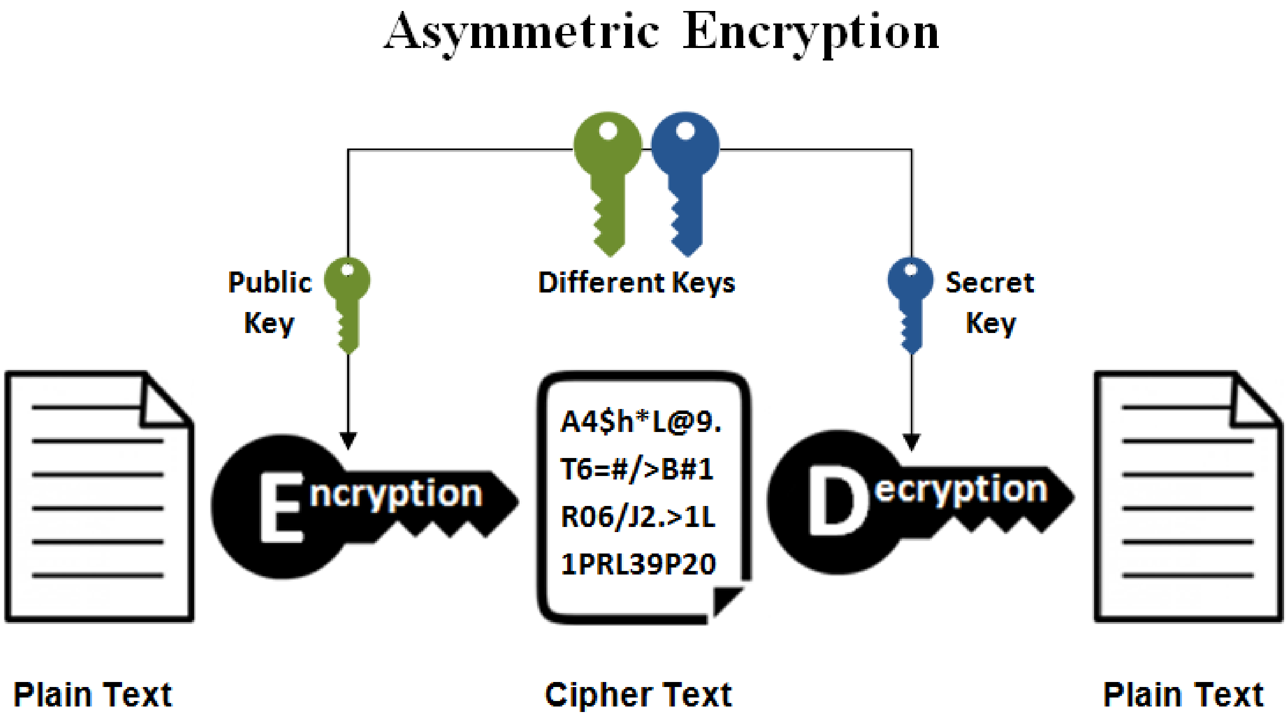
Wer den **Public Key** hat, kann **Daten verschlüsseln**, die nur die Person mit **Private Key lesen** kann. Wer den **Private Key** hat, kann **Daten verschlüsseln**, die jede Person mit **Public Key lesen** kann.

Symmetrische Verschlüsselung:
Ein Schlüssel (**Private Key / Secret Key**)



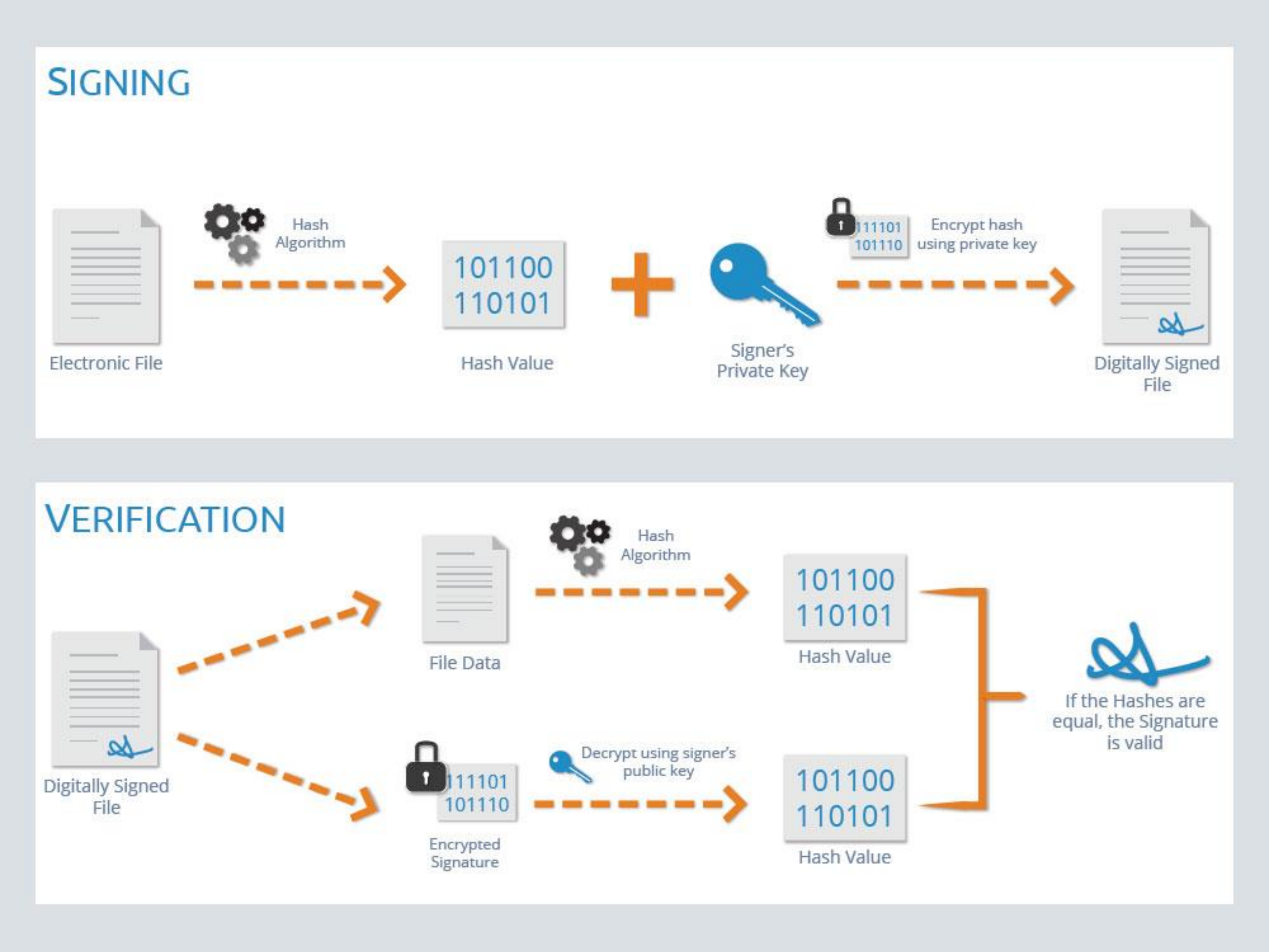
Wer den **Schlüssel** hat, kann **Daten verschlüsseln** und **lesen**.
Nur sinnvoll für die **eigene Datenspeicherung**.
Eine **Person** kann sehr **viele Schlüssel** generieren.

Asymmetrische Verschlüsselung:
Zwei Schlüssel (**Private Key** und **Public Key**)



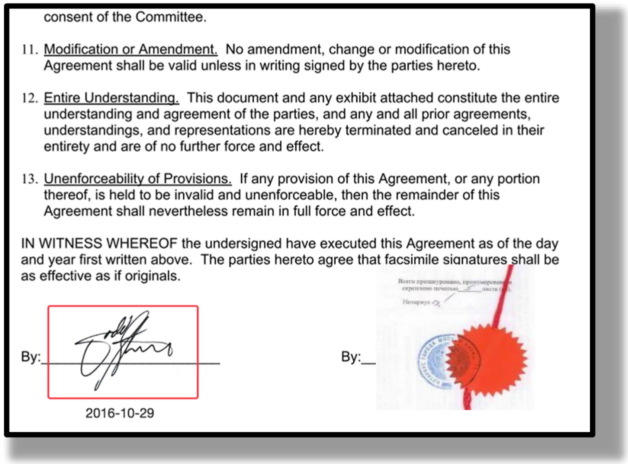
Wer den **Private oder Public Key** hat, kann **Daten verschlüsseln**.
Wer den anderen **Key vom Schlüsselpaar** hat, kann **Daten lesen**.
Eine **Person** kann sehr **viele Schlüsselpaare** generieren.

Digital signiertes Dokument (für Bitcoin relevant)



Signierte vs digital signierte Dokumente

Signiertes Dokument:



consent of the Committee.

11. Modification or Amendment. No amendment, change or modification of this Agreement shall be valid unless in writing signed by the parties hereto.

12. Entire Understanding. This document and any exhibit attached constitute the entire understanding and agreement of the parties, and any and all prior agreements, understandings, and representations are hereby terminated and canceled in their entirety and are of no further force and effect.

13. Unenforceability of Provisions. If any provision of this Agreement, or any portion thereof, is held to be invalid and unenforceable, then the remainder of this Agreement shall nevertheless remain in full force and effect.

IN WITNESS WHEREOF the undersigned have executed this Agreement as of the day and year first written above. The parties hereto agree that facsimile signatures shall be as effective as if originals.

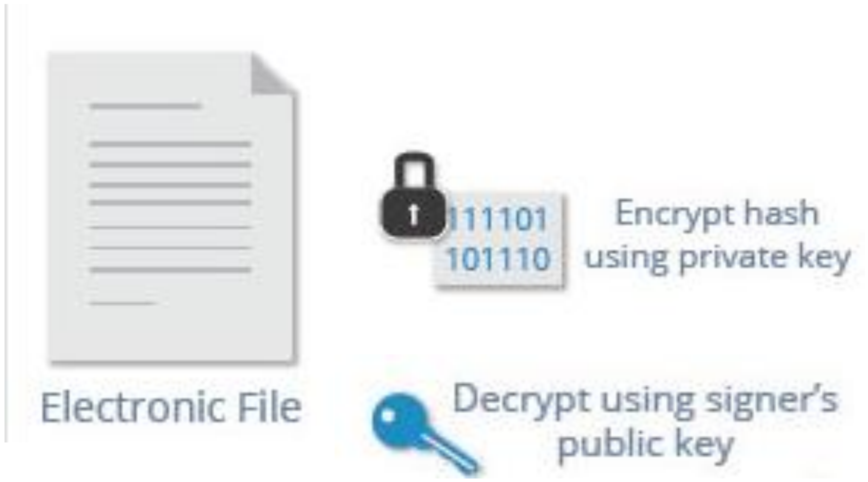
Всего прошнуровано, пронумеровано и скреплено печатью 5 листа (ов).
Нотариус

By:

2016-10-29

By:

Digital signiertes Dokument:


111101
101110
Encrypt hash using private key
Electronic File
Decrypt using signer's public key

Ein signiertes Dokument benötigt:

- **Dokument**
- **Unterschrift** (Signature)

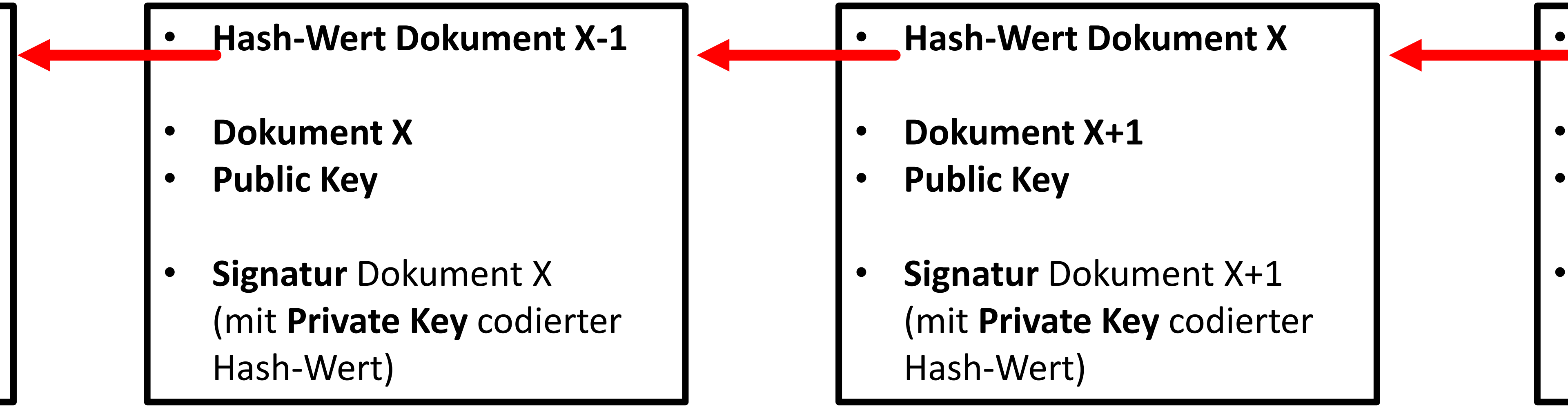
- (Notarielle Beglaubigung)

Ein digital signiertes Dokument benötigt:

- **Dokument** (lesbar)
- **Signatur** (mit **Private Key** codierter **Hash-Wert**)
- **Public Key**

Kette von digital signierten Dokumenten

(für Bitcoin relevant)



Digital signiertes Dokument X:

- **Hash-Wert Dokument X-1**
- **Dokument X**
- **Public Key**
- **Signatur** Dokument X (mit **Private Key** codierter Hash-Wert)

Digital signiertes Dokument X+1:

- **Hash-Wert Dokument X**
- **Dokument X+1**
- **Public Key**
- **Signatur** Dokument X+1 (mit **Private Key** codierter Hash-Wert)

Die **Signatur** bezieht sich auf das **Gesamtdokument** und umfasst den **Hash-Wert** vom **Vordokument** und den **Public Key**.

Bei **Änderung** eines **Vordokumentes** müssen alle **Folgedokumente** auch geändert werden (**Reihenfolge** der Dokumente ist festgelegt).

How a Ƀitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

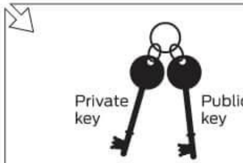
Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.



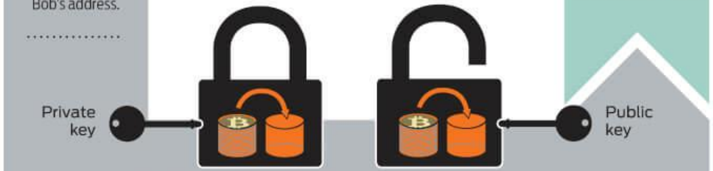
Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

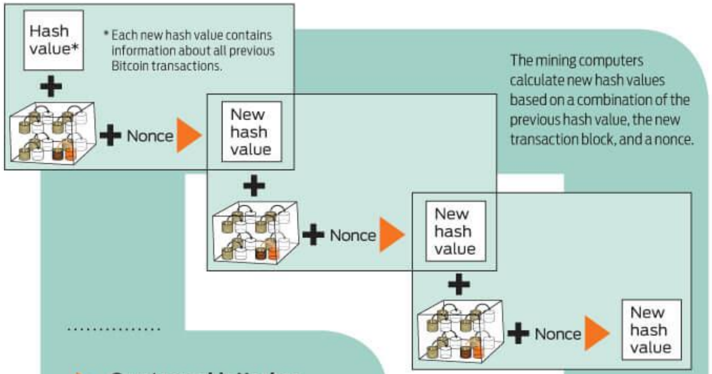
Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.



* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all euil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

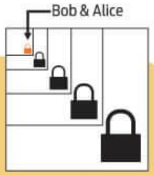
The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED



As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.