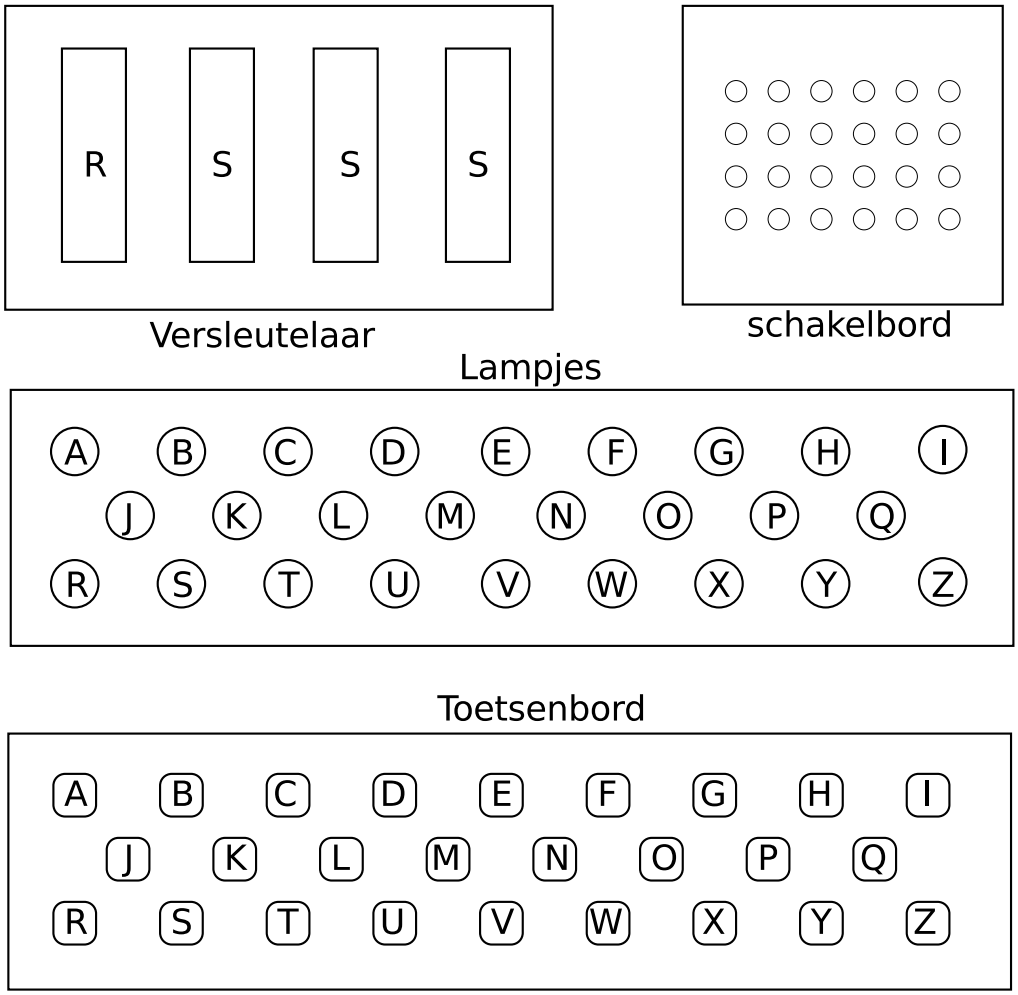
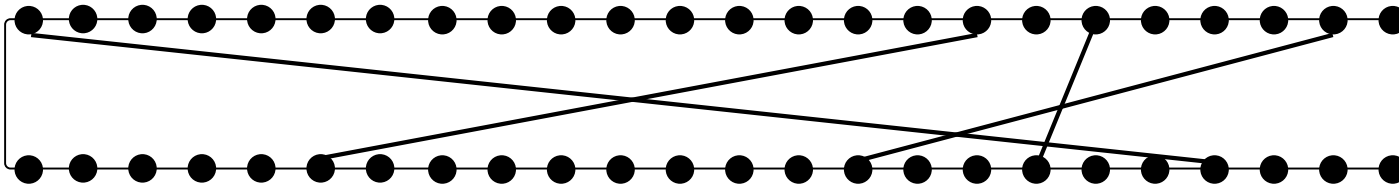
Hoofdstuk 17

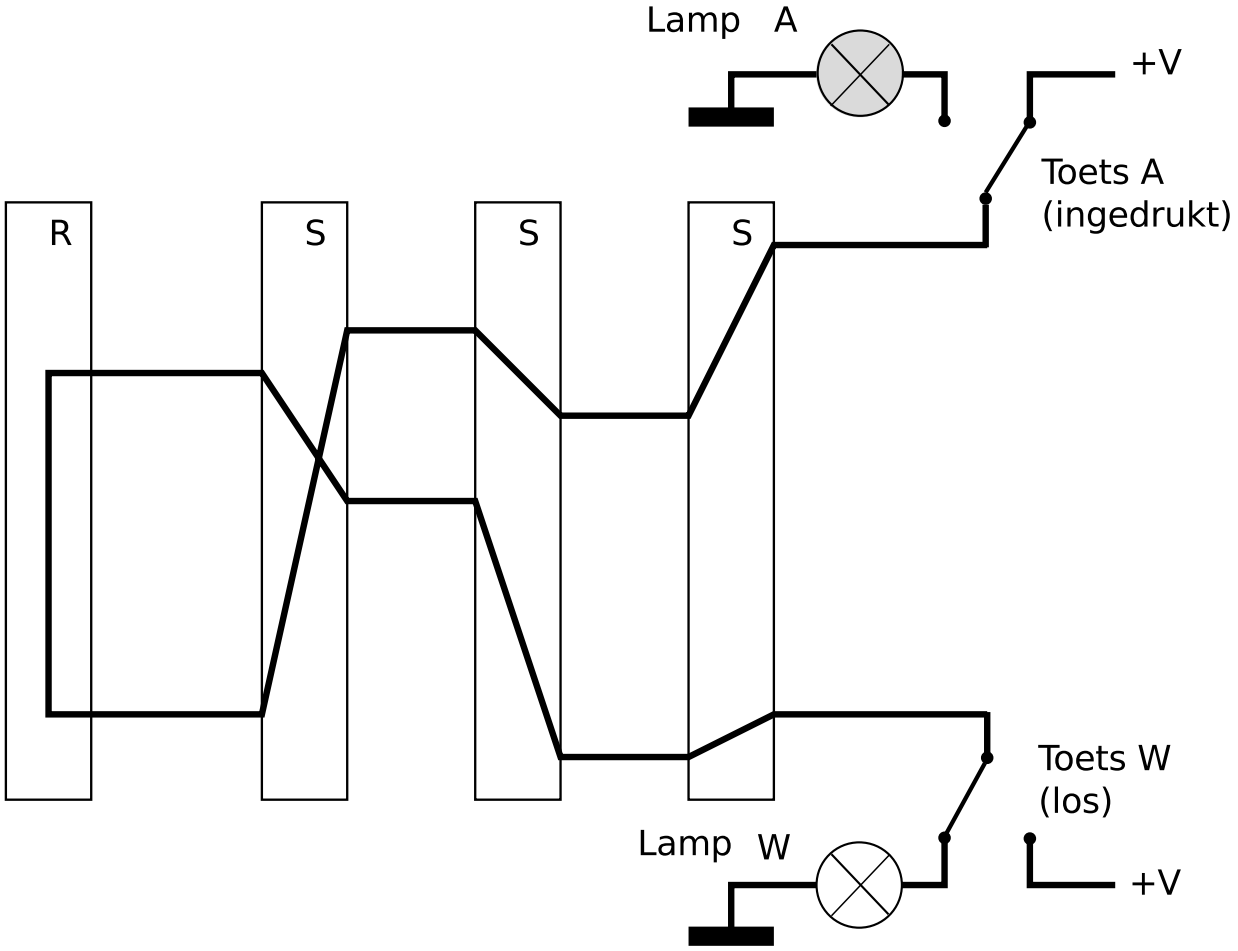
Security



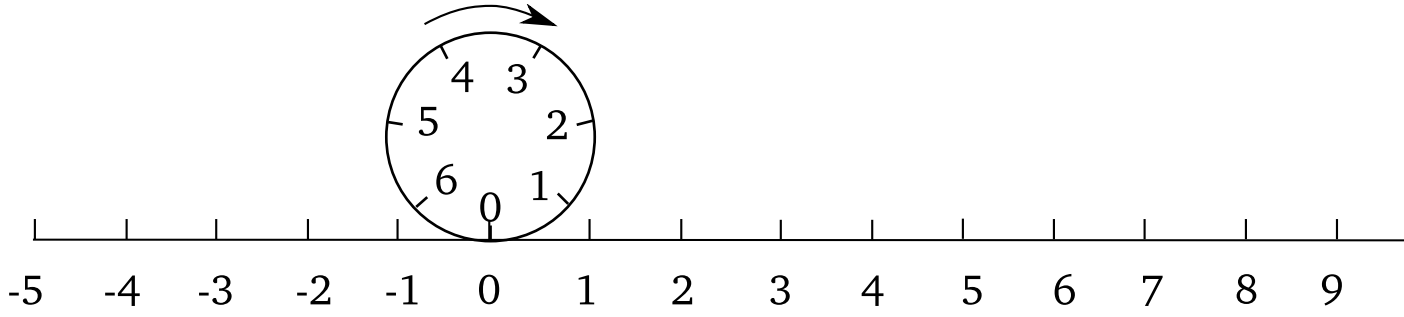
Figuur 17.1: Bouwstenen van de enigma.



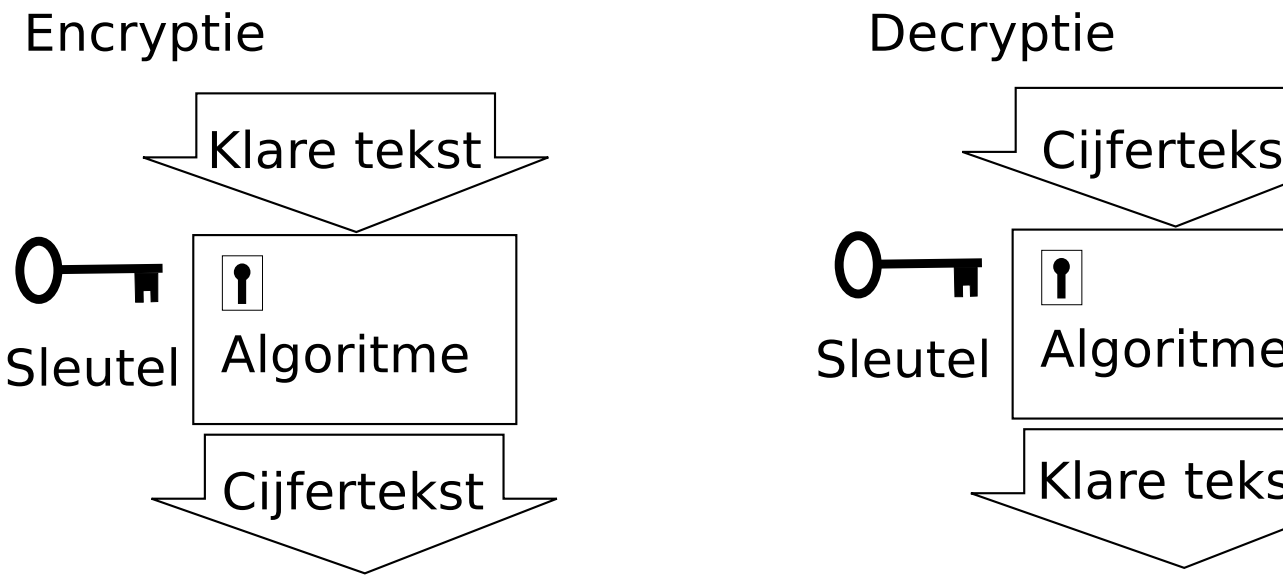
Figuur 17.2: Een scrambler van de enigma.



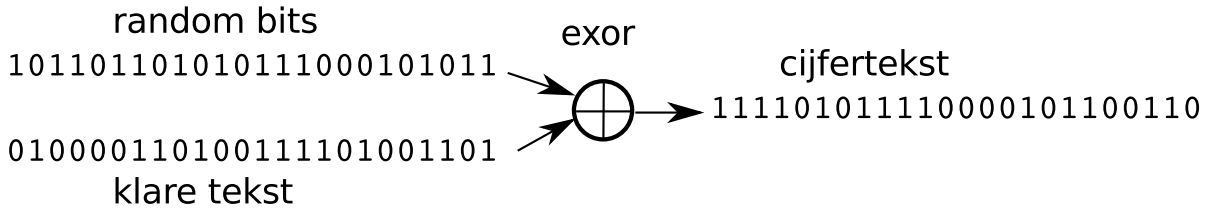
Figuur 17.3: Werking van de enigma.



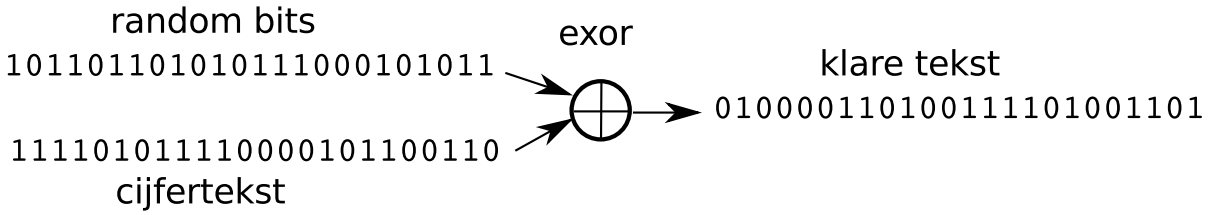
Figuur 17.4: Modulus 7 gevisualiseerd.



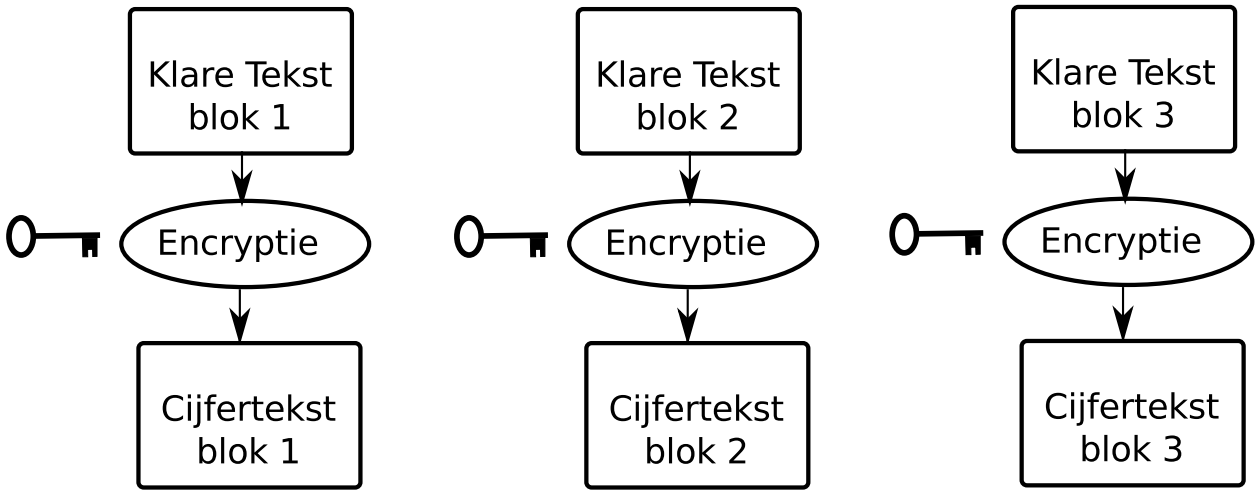
Figuur 17.5: Symmetrische encryptie en decryptie.



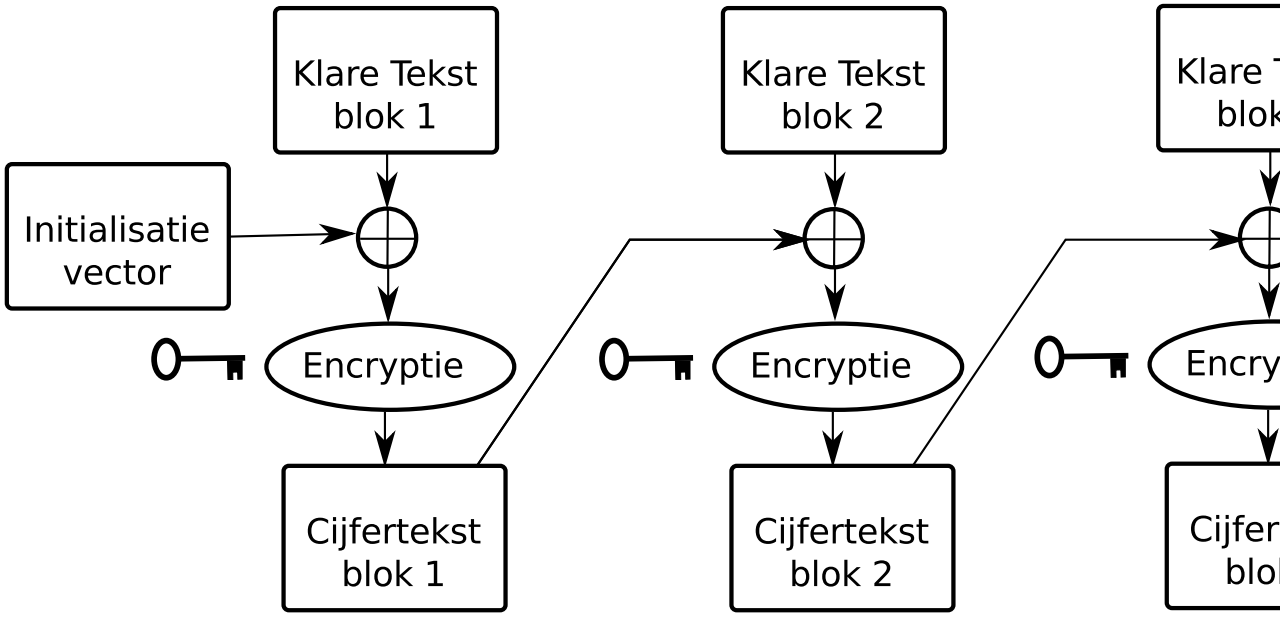
Figuur 17.6: OTP-encryptie.



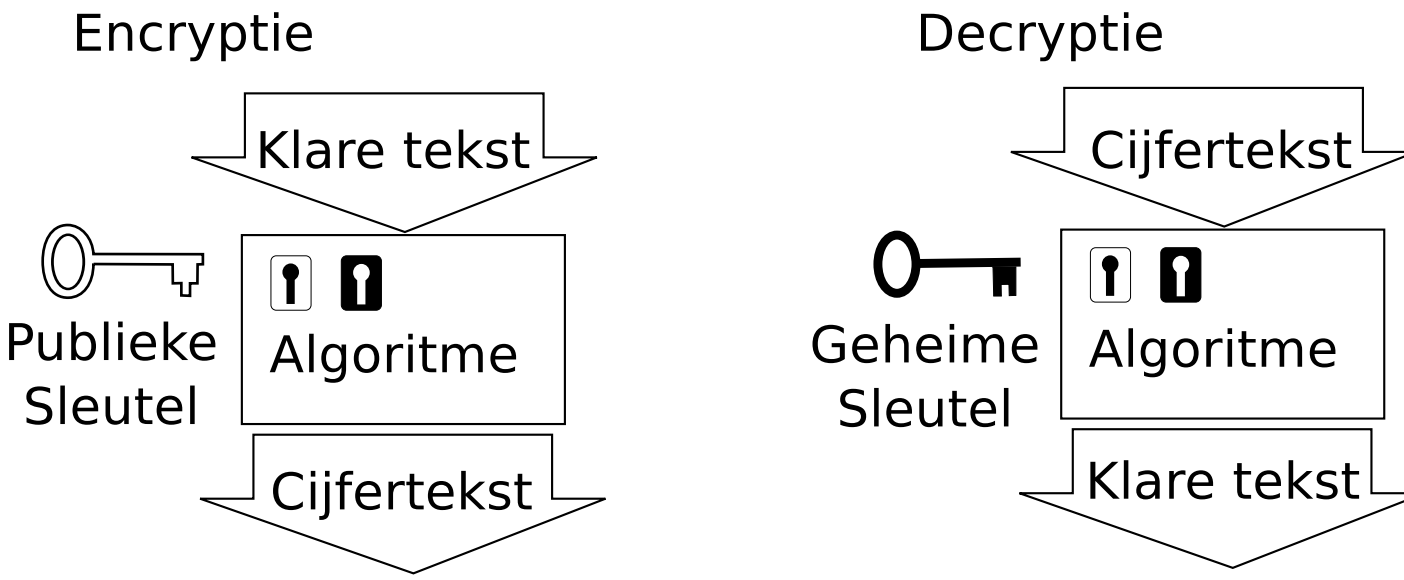
Figuur 17.7: OTP-decryptie.



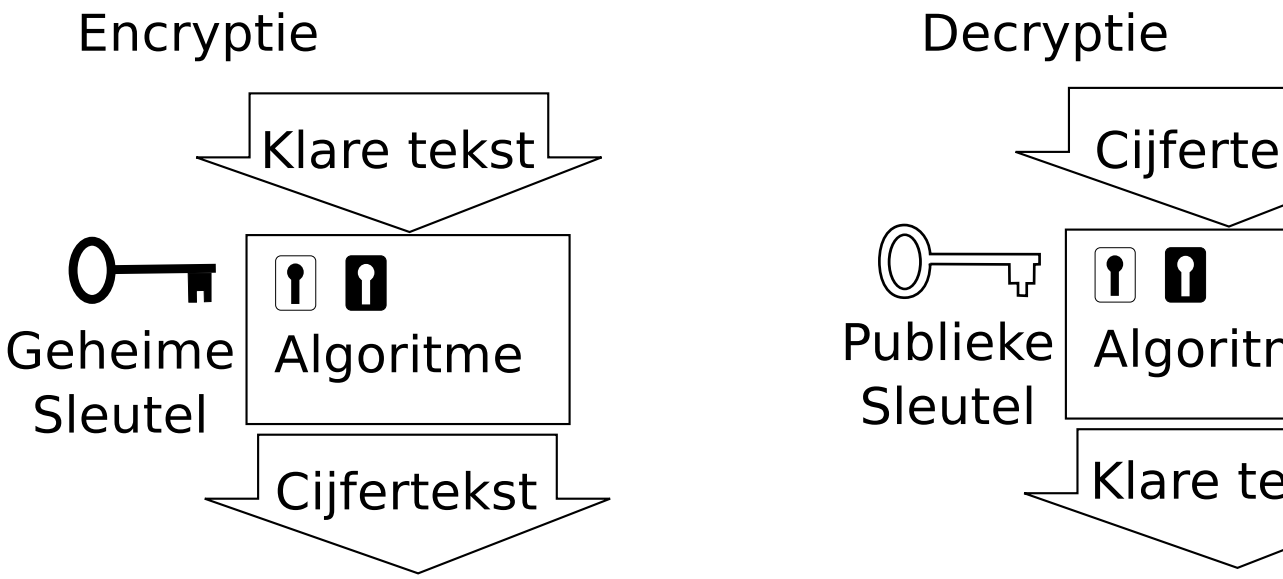
Figuur 17.8: Electronic code book.



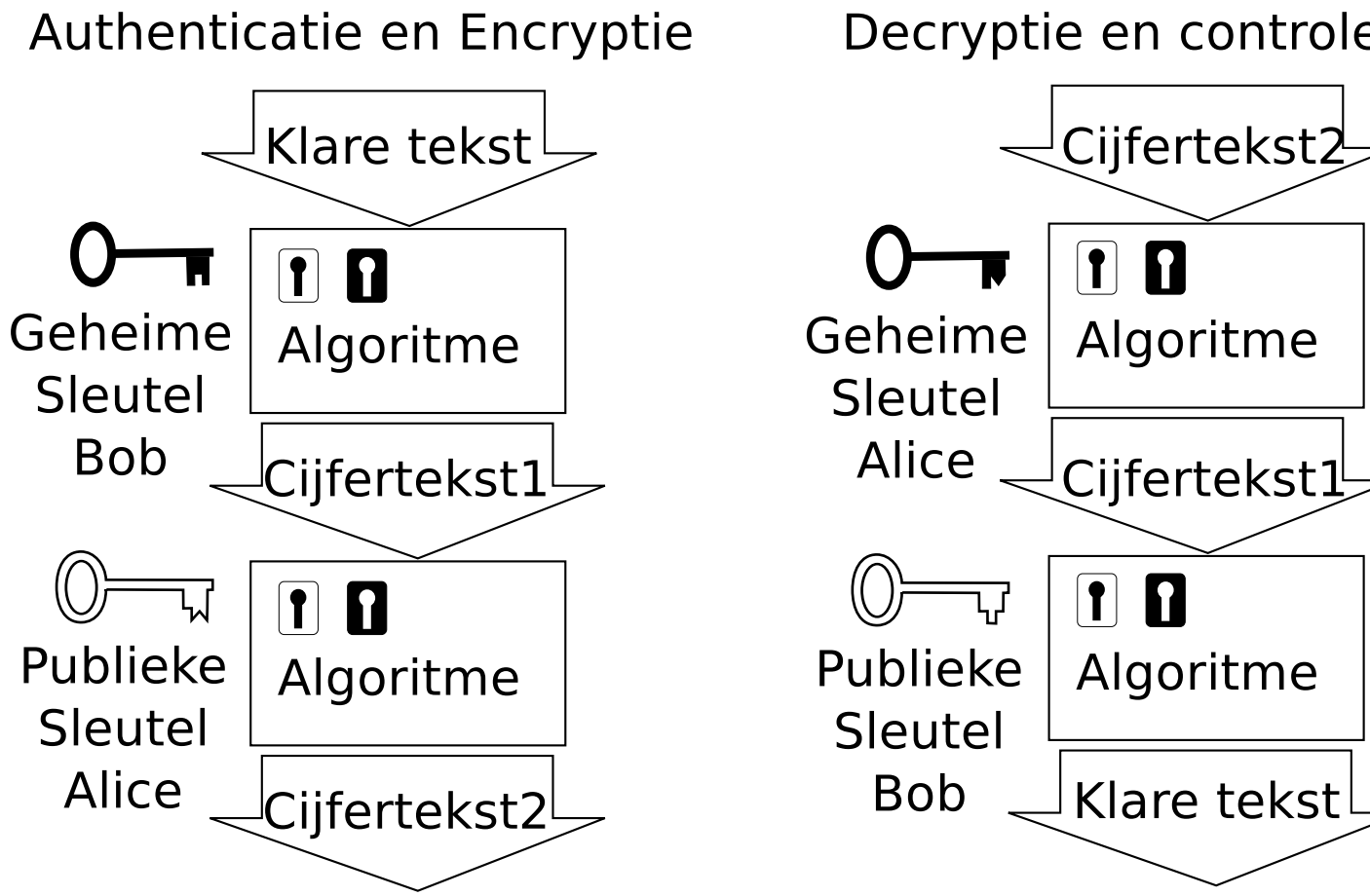
Figuur 17.9: Cipher block chaining.



Figuur 17.10: Asymmetrische encryptie en decryptie.



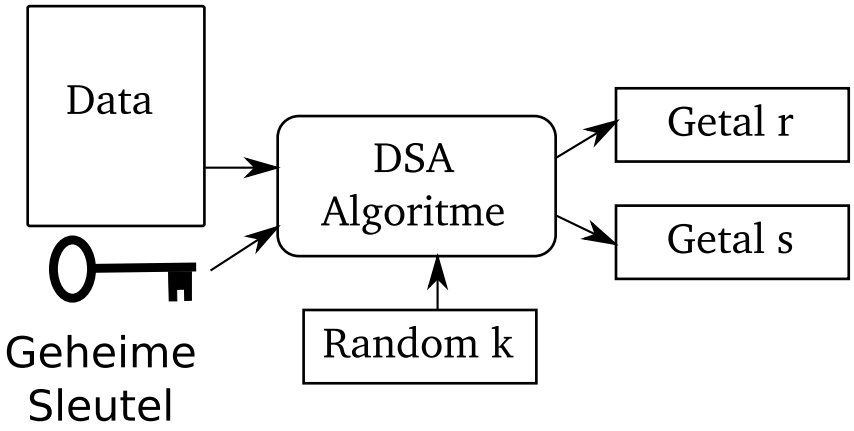
Figuur 17.11: Authenticatie bij asymmetrische encryptie.



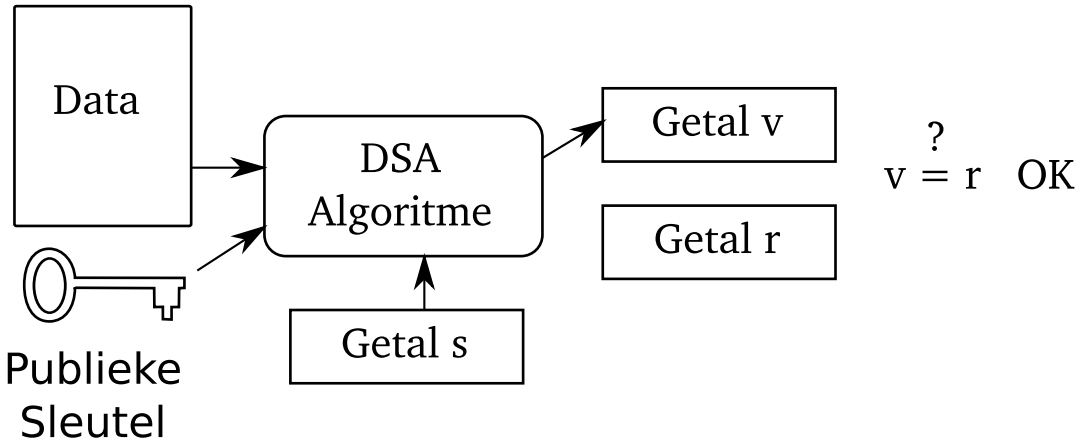
Figuur 17.12: Authenticatie en encryptie gecombineerd.

ha	`925cc8d2953eba624b2bfedf91a91613`
hal	`cde9e8dec3ca8de88aa6cf61c1c0252c`
hallo	`598d4c200461b81522a3328565c25f7c`
hello	`5d41402abc4b2a76b9719d911017c592`

Figuur 17.13: MD5 hashes voor vier verschillende teksten.



Figuur 17.14: Ondertekening van een bericht met DSA.



Figuur 17.15: Verificatie van een ondertekening met DSA.