13-4 ATTACKS ON DIGITAL SIGNATURE

This section describes some attacks on digital signatures and defines the types of forgery.

Topics discussed in this section:

13.18

13.4.1 Attack Types

Key-Only Attack — Attacker only knows the public key of the signer

Known-Message Attack — Attacker knows one or more Message Signature pairs

Chosen-Message Attack — Attacker chooses one or more Messages, and convinces the signer to sign those (generate signatures for those messages)

13.19

13.4.2 Forgery Types

Existential Forgery — Attacker successfully creates a *valid* message-signature pair, but the message is syntactically/ semantically meaningless

Selective Forgery — Attacker selects the message contents, and manages to get Alice's signature on it

13.20

13-5 DIGITAL SIGNATURE SCHEMES

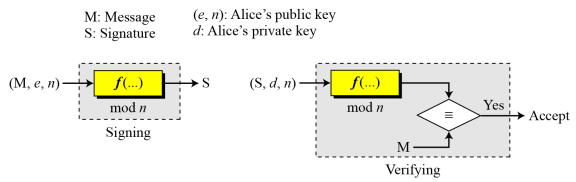
Several digital signature schemes have evolved during the last few decades. Some of them have been implemented.

Topics discussed in this section:

13.21

13.5.1 RSA Digital Signature Scheme

Figure 13.6 *General idea behind the RSA digital signature scheme*



13.22

13.5.1 Continued

Key Generation

Key generation in the RSA digital signature scheme is exactly the same as key generation in the RSA

Note

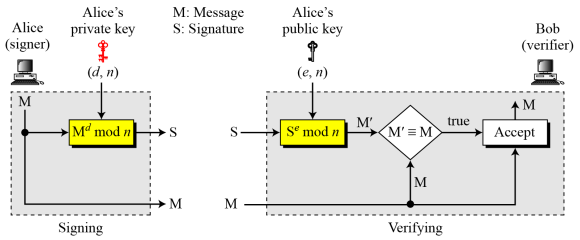
In the RSA digital signature scheme, *d* is private; *e* and *n* are public.

13.23

13.5.1 Continued

Signing and Verifying

Figure 13.7 *RSA digital signature scheme*



13.24

13.5.1 Continued

Example 13.1

As a trivial example, suppose that Alice chooses $p = 823$ and $q = 953$, and calculates $n = 784319$. The value of $\phi(n)$ is 782544. Now she chooses $e = 313$ and calculates $d = 160009$. At this point key generation is complete. Now imagine that Alice wants to send a message with the value of M = 19070 to Bob. She uses her private exponent, 160009, to sign the message:

$$\text{M: } 19070 \rightarrow \text{S} = (19070^{160009}) \bmod 784319 = 210625 \bmod 784319$$

Alice sends the message and the signature to Bob. Bob receives the message and the signature. He calculates

$$M' = 210625^{313} \bmod 784319 = 19070 \bmod 784319 \rightarrow M \equiv M' \bmod n$$

Bob accepts the message because he has verified Alice's signature.

13.25

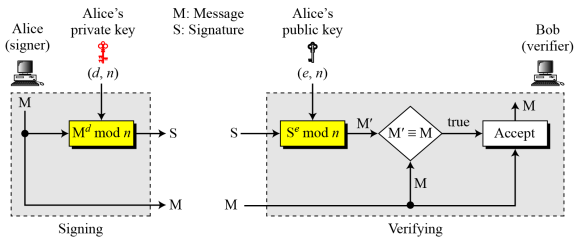
Attacks on RSA Digital Signature

Key-Only Attack on RSA DSS:

Eve intercepts (M,S)

Eve tries to find another M' such that $M' \equiv S^e \pmod n$ ⇐ ***Difficult due to DLP hardness***

Eve sends (M',S) to Bob, posing as Alice



13.26

Attacks on RSA Digital Signature

Known-Message Attack on RSA DSS:

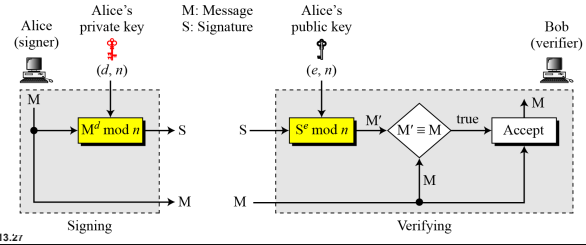
Eve intercepts (M1,S1) and (M2,S2)

Eve sends (M,S) to Bob, posing as Alice ⇐ **M is possibly meaningless! (*Example of Existential forgery*)**

where M = M1×M2

and S = S1×S2

Works since $S = S1 \times S2 = M1^d \bmod n \times M2^d \bmod n = (M1 \times M2)^d \bmod n = M^d \bmod n$



13.27

Attacks on RSA Digital Signature

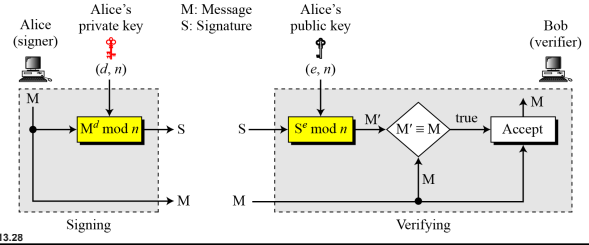
Chosen-Message Attack on RSA DSS:

Eve ***selects*** (M1,S1) and (M2,S2) such that M1×M2 = (meaningful) M

Eve sends (M,S) to Bob, posing as Alice ⇐ **M is chosen! (*Example of Selective forgery*)**

where S = S1×S2

Works again! Additionally M is meaningful!

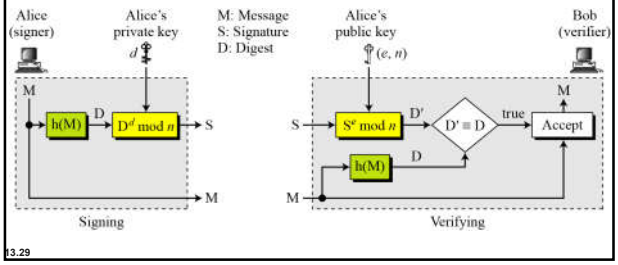


13.28

13.5.1 Continued

RSA Signature on the Message Digest

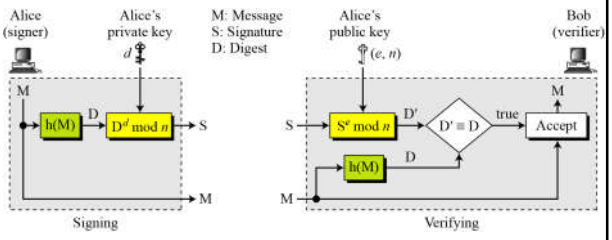
Figure 13.8 *The RSA signature on the message digest*



13.29

Attacks on RSA Signature on Message Digest

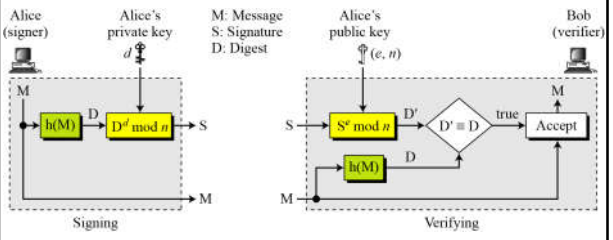
Key-Only Attack:
Eve intercepts (M,S) and tries to find M' such that h(M) = h(M') ***Preimage Attack***
Eve sends (M',S) to Bob, posing as Alice



13.30

Attacks on RSA Signature on Message Digest

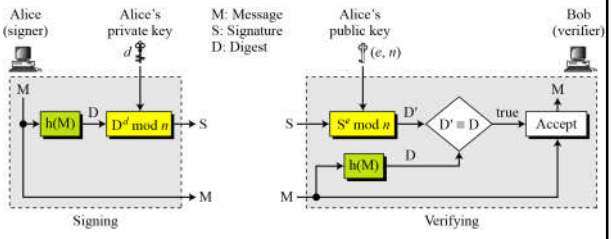
Key-Only Attack:
Eve finds a digest D and its signature S. Eve tries to find M' such that h(M') = D ***Preimage Attack***
Eve sends (M',S) to Bob, posing as Alice



13.31

Attacks on RSA Signature on Message Digest

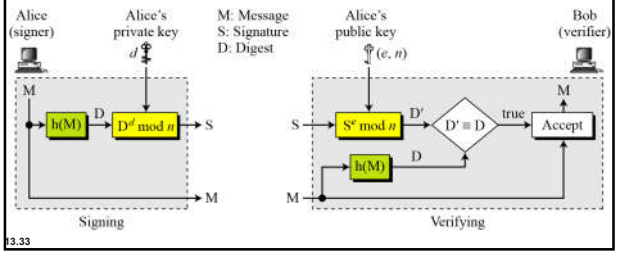
Key-Only Attack:
Eve has two messages M and M' such that h(M) = h(M') ***Collision Attack***
Eve convinces Alice to sign M and generate S
Eve sends (M',S) to Bob, posing as Alice



13.32

Attacks on RSA Signature on Message Digest

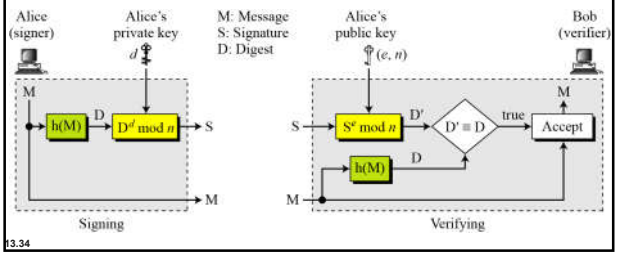
Known-Message Attack:
Eve intercepts (M1,S1) and (M2,S2)
Eve computes S = S1×S2
Eve can compute h(M) = h(M1)×h(M2), such that signature of h(M) is S=S1×S2
Eve wants to send (M,S) to Bob posing as Alice
Eve tries to find M from h(M) ⟸ ***Preimage attack***



13.33

Attacks on RSA Signature on Message Digest

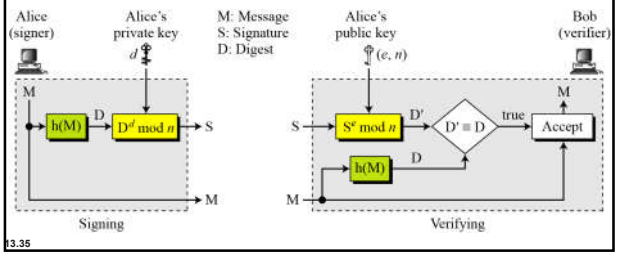
Chosen-Message Attack:
Eve selects a message M, to send to Bob posing as Alice. Eve computes h(M).
Eve decomposes h(M) into h(M) = h(M1)×h(M2)
Eve needs to convince Alice to sign M1,M2, to have S1,S2, so that Eve can send (M,S1×S2) to Bob posing as Alice, because signature of h(M) is S1×S2
Eve tries to find M1,M2 from h(M1),h(M2) ⟸ ***Preimage attack***



13.34

Attacks on RSA Signature on Message Digest

Chosen-Message Attack:
Eve selects two meaningful messages M1 and M2, and convinces Alice to sign M1,M2, to have S1,S2 respectively
Signature of h(M) = h(M1)×h(M2) is S1×S2
Eve can send (M, S1×S2) to Bob posing as Alice, if Eve can find M from h(M)
⟸ ***Preimage attack***



13.35