Digital Signature

Objectives

- To define a digital signature
- To define security services provided by a digital signature
- To define attacks on digital signatures
- To discuss some digital signature schemes, including RSA, ElGamal,
- Schnorr, DSS, and elliptic curve
- To describe some applications of digital signatures

ATTACKS ON DIGITAL SIGNATURE

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

Topics discussed in this section:

13.4.1 **Attack Types**

13.4.2 **Forgery Types**

13.4.1 Attack Types

Key-Only Attack

the attacker is only given the public verification key.

Known-Message Attack

the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker.

Chosen-Message Attack

the attacker first learns signatures on arbitrary messages of the attacker's choice.

13.4.2 Forgery Types

Existential Forgery

Existential forgery is the creation (by an adversary) of any message/signature pair (m,σ), where σ was not produced by the legitimate signer.

Selective Forgery

Selective forgery is the creation (by an adversary) of a message/signature pair (*m*,σ) **where *m* has been *chosen* by the adversary prior to the attack.**

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:

RSA Digital Signature Scheme
ElGamal Digital Signature Scheme
Schnorr Digital Signature Scheme
Digital Signature Standard (DSS)
Elliptic Curve Digital Signature Scheme

Key Generation

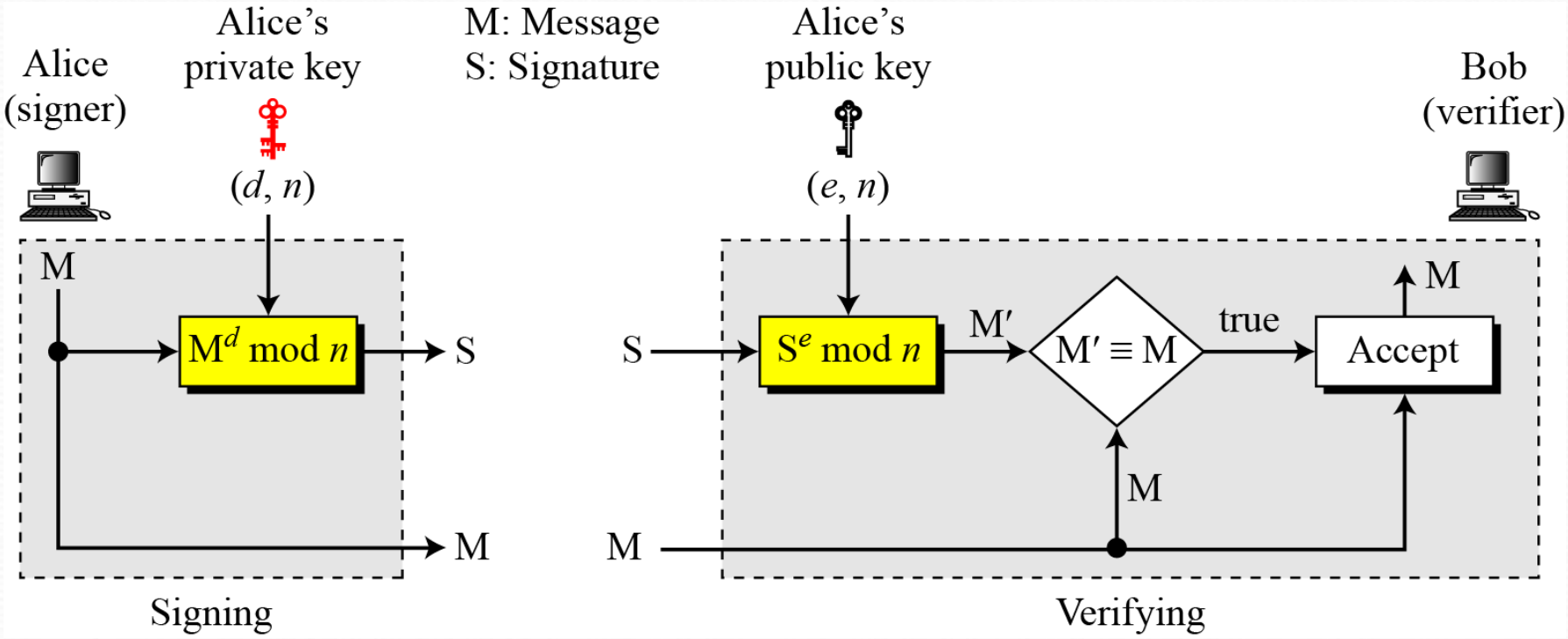
Key generation in the RSA digital signature scheme is exactly the same as key generation in the RSA

Note

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

Signing and Verifying

Figure 13.7 ***RSA digital signature scheme***

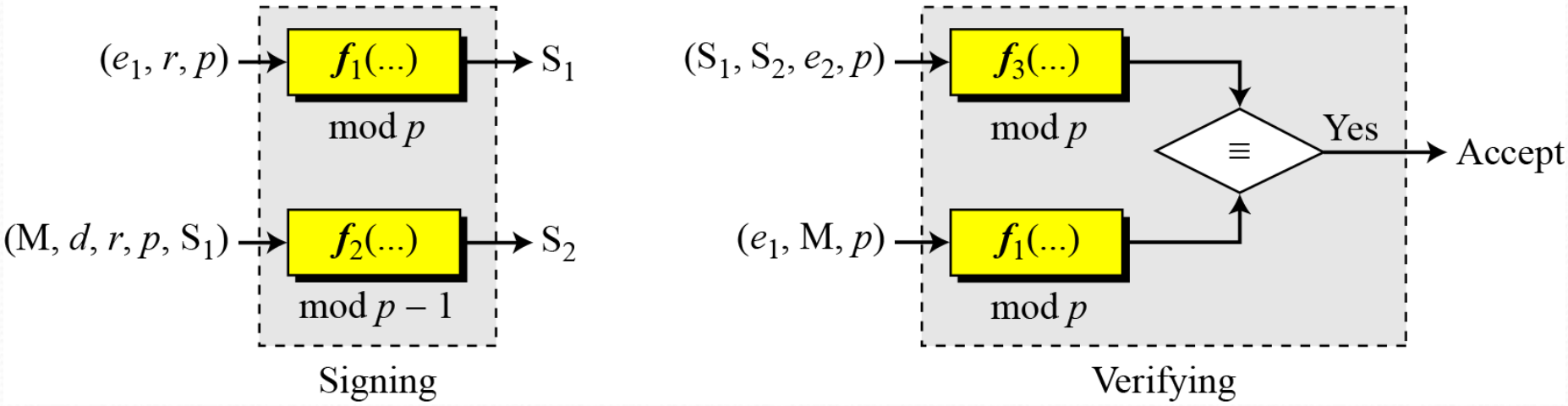


ElGamal Digital Signature Scheme

General idea behind the ElGamal digital signature scheme

S_1, S_2: Signatures
M: Message
(e_1, e_2, p): Alice's public key

d: Alice's private key
r: Random secret



Key Generation

The key generation procedure here is exactly the same as the one used in the cryptosystem.

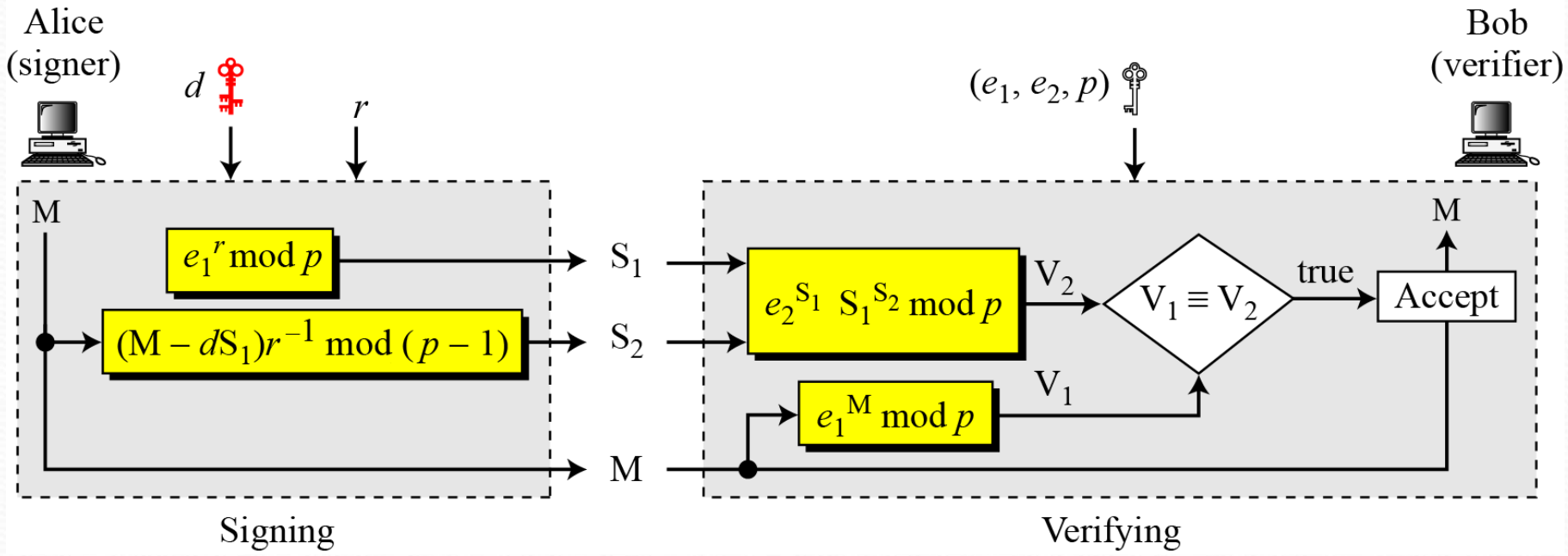
Note

In ElGamal digital signature scheme, (e_1, e_2, p) is Alice's public key; d is her private key.

Verifying and Signing

Figure 13.10 *ElGamal digital signature scheme*

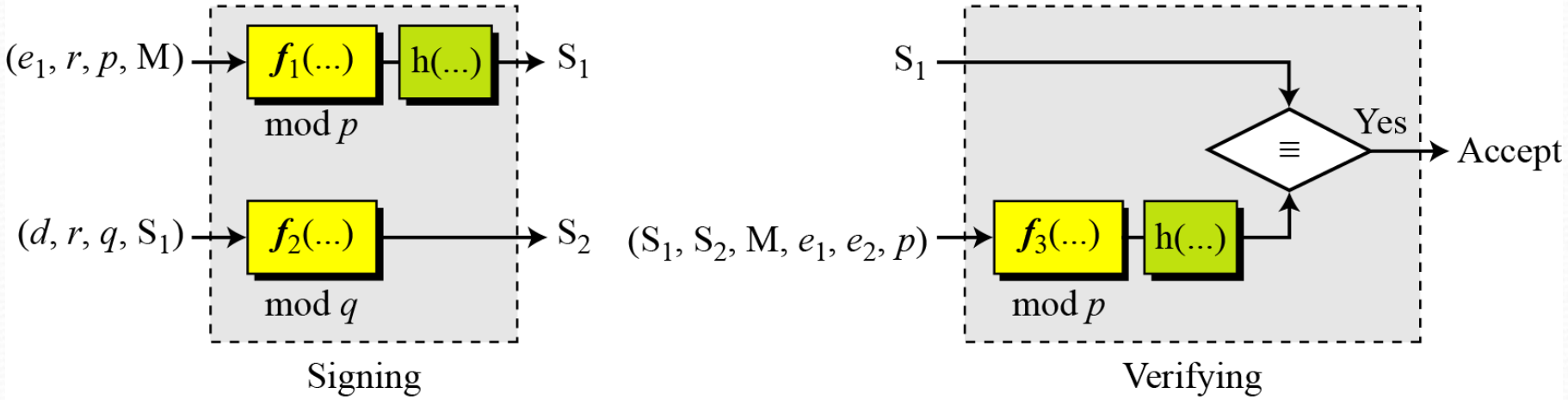
M: Message
S_1, S_2: Signatures
V_1, V_2: Verifications
r: Random secret
d: Alice's private key
(e_1, e_2, p): Alice's public key



Schnorr Digital Signature Scheme

General idea behind the Schnorr digital signature scheme

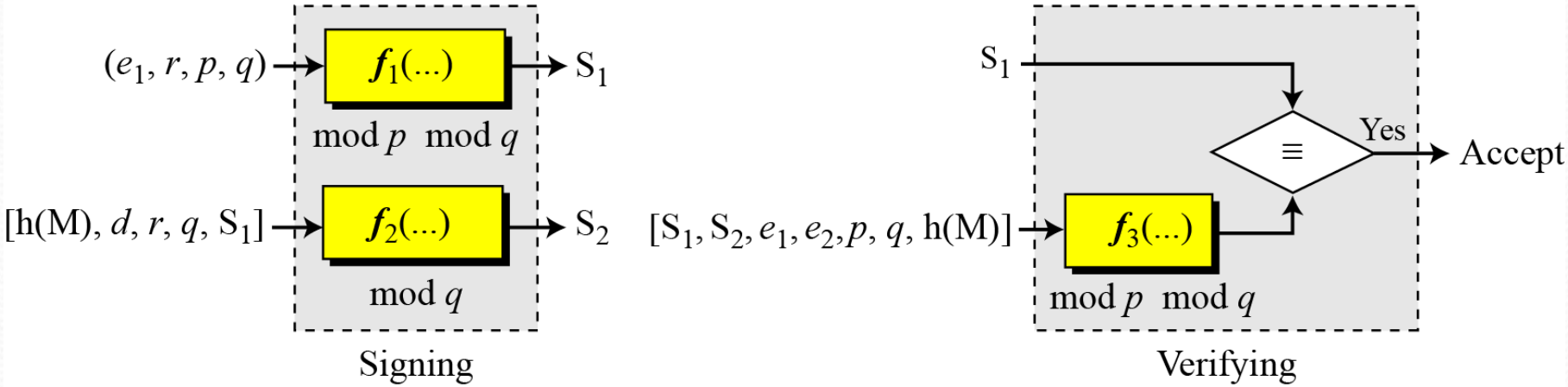
S_1, S_2: Signatures
M: Message
(e_1, e_2, p, q): Alice's public key
(d): Alice's private key
r: Random secret



Digital Signature Standard (DSS)

General idea behind DSS scheme

S_1, S_2: Signatures
M: Message
(e_1, e_2, p, q): Alice's public key
d: Alice's private key
r: Random secret



DSS Versus RSA

Computation of DSS signatures is faster than computation of RSA signatures when using the same p.

DSS Versus ElGamal

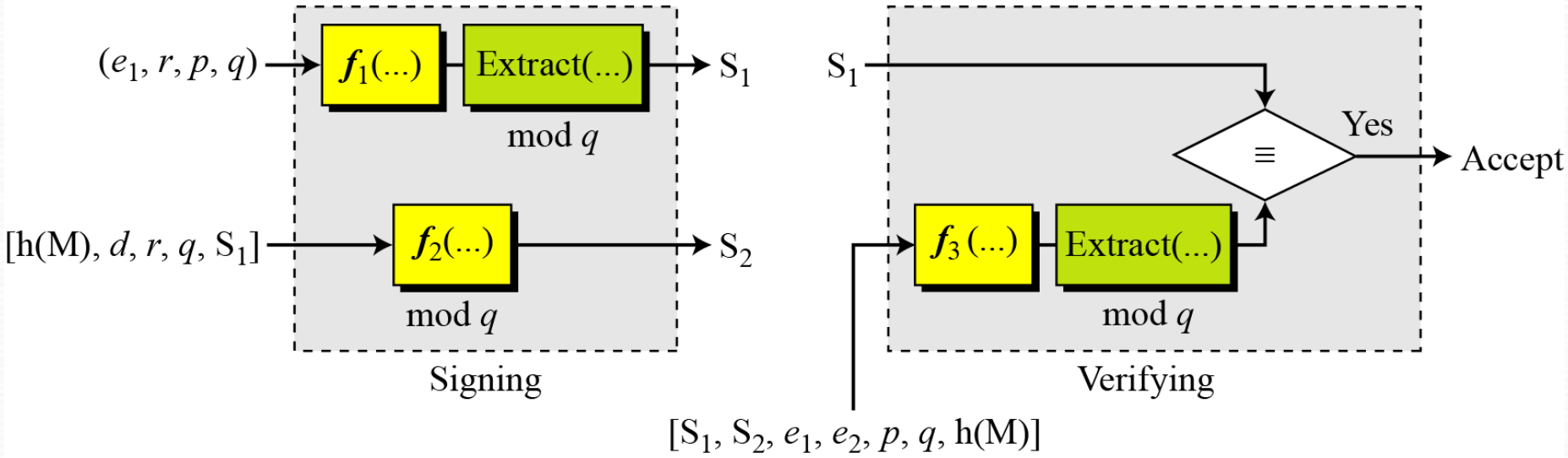
DSS signatures are smaller than ElGamal signatures because q is smaller than p.

Elliptic Curve Digital Signature Scheme

General idea behind the ECDSS scheme

S_1, S_2: Signatures
M: Message
(a, b, p, q, e_1, e_2): Alice's public key

d: Alice's private key
r: Random secret



VARIATIONS AND APPLICATIONS

This section briefly discusses variations and applications for digital signatures.

Topics discussed in this section:

Variations
Applications

Variations

Time Stamped Signatures

Sometimes a signed document needs to be time stamped to prevent it from being replayed by an adversary. This is called time-stamped digital signature scheme.

Blind Signatures

Sometimes we have a document that we want to get signed without revealing the contents of the document to the signer.