CHAPTER 13

Digital Signature

(Solution to Odd-Numbered Problems)

Review Questions

1. We mentioned four areas in which there is a differences between a conventional and a digital signature: inclusion, verification, document-signature relation, and duplicity.

a. **Inclusion**: a conventional signature is included in the document; a digital signature is a separate document.

b. **Verification**: A conventional signature is verified by comparing with the signature on file. The verifier of a digital signature needs to create a new signature.

c. **Relation:** A document and a conventional signature has a one-to-many relation; a message and a digital signature has one-to-one relation.

d. **Duplicity:** In conventional signature, a copy of the signed document can be distinguished from the original one on file. In digital signature, there is no such distinction unless there is a factor of time (such as a timestamp) on the document.

3. The following table shows the relationship between attacks on a cryptosystem and attacks on a digital signature.

Cryptosystem attacks	***Digital signature Attacks***
Ciphertext-only	Key-only
Known-plaintext	Known-message
Chosen-plaintext	Chosen-message
Chosen-ciphertext	▨

5. The idea behind the RSA digital signature scheme is the same as the RSA cryptosystem, but the roles of the private and public keys are changed. First, the private and public keys of the sender, not the receiver, are used. Second, the sender uses her own private key to sign the document; the receiver uses the sender's public key to verify it.

7. The Schnorr digital signature scheme is similar the ElGamal digital signature but the size of the signatures are smaller.

9. The elliptic curve digital signature scheme is based on DSA, but uses elliptic curves. The scheme is similar to the elliptic curve cryptosystem in which the signer and verifiers manipulate points on an elliptic curve.

Exercise

11. We have $n = 809 \times 751 = 607559$ $\phi(n) = (809 - 1) \times (751 - 1) = 606000$. Since d = 23, we have $e = d^{-1} \bmod \phi(n) = 158087$.

   a. We have

$$S_1 = M_1^{d} \bmod n = 100^{23} \bmod 607559 = 223388$$
$$M_1 = S_1^{e} \bmod n = 223388^{158087} \bmod 607559 = 100$$

   b. We have

$$S_2 = M_2^{d} \bmod n = 50^{23} \bmod 607559 = 5627$$
$$M_2 = S_2^{e} \bmod n = 5627^{158087} \bmod 607559 = 50$$

   c. If $M = M_1 \times M_2 = 5000$, we have

$$S = M^{d} \bmod n = 5000^{23} \bmod 607559 = \mathbf{572264}$$
$$S = (S_1 \times S_2) \bmod n = (223388 \times 5627) \bmod 607559 = \mathbf{572264}$$

13. We have $q = 83$, $p = 997$, and $d = 23$. We choose $e_0 = 7$. Then $e_1 = e_0^{(p-1)/q} \bmod p = 9$ $e_2 = e_1^{d} \bmod p = 521$. We calculate S_1 and S_2 in mod q. We let h(40067) = 81 (The actual value does not matter here).

$$S_1 = h(M \mid e_1^{r} \bmod p) = h(400 \mid 9^{11} \bmod p) = h(400 \mid 67) = h(40067) = \mathbf{81}$$

$$S_2 = r + ds_1 \bmod q = 11 + 23 \times 81 \bmod 83 = \mathbf{48}$$

We can verify the signature assuming that h(40067) = 81.

$$V = h(M \mid e_1^{S_2} e_2^{-S_1} \bmod p) = h(400 \mid 9^{48}\, 521^{-81} \bmod 997) =$$

$$V = h(400 \mid 9^{48}\, 521^{2} \bmod 997) = h(400 \mid 877 \times 257 \bmod 997) =$$

$$V = h(400 \mid 67) = h(40067) = \mathbf{81}$$

15.

   a. In RSA scheme $S = M^{d} \bmod n$. This means that the value of S can be as large as $(n - 1)$. In other words the size of $|S| \approx |n| \approx 1024$ bits.

b. In ElGamal scheme $S_1 = (\ldots) \bmod p$ and $S_2 = (\ldots) \bmod (p - 1)$. This means that the value of S_1 can be as large as $(p - 1)$ and the value of S_2 can be as large as $(p - 2)$ In other words the size of $|S_1| \approx |p| \approx 1024$ bits and the size of $|S_2| \approx |p| \approx 1024$ bits. This means the sign of the signature is 2048 bits.

c. In Schnorr scheme $S_1 = h (...)$ and $S_2 = (\ldots) \bmod (q)$. This means that the value of S_1 is exactly equals $h (...)$ and the value of S_2 can be as large as $(q - 1)$. Since q is required to be the same size as q. The size of $|S_1| \approx |q| \approx 160$ bits and the size of $|S_2| \approx |q| \approx 160$ bits. This means the sign of the signature is 320 bits. The signature in Schnorr is much smaller than signature in ElGamal.

d. In DSS scheme $S_1 = (\ldots) \bmod q \quad S_2 = (\ldots) \bmod q$. This means that the value of S_1 and S_2 can be as large as $(q - 1)$. The size of $|S_1| = |S_2| \approx |q| \approx 160$ bits and the This means the sign of the signature is 320 bits. The signature in DSS is the same size as the signature in the Schnorr scheme.

17. In all of these schemes, Eve can calculate the value of d if she intercept a message and its signature. She can then forge a message from Alice to Bob. Each case is described separately in Exercises 23, 24, and 25.

19. If $p = 19$ and $q = 3$, $n = 57$. Eve can easily calculate $\phi(n) = \phi(57) = 36$. Since e is public, Eve can find $d = e^{-1} \bmod n$. Eve can now choose a message of her own M, calculate $S = M^d \bmod n$. Eve then sends M and S to Bob and pretends that they are coming from Alice.

21. If $p = 29$ and $q = 7$, then the value of d is between 2 and 7 (it should be less than $q - 1$). Since $e_2 = e_1^{\mathrm{d}} \bmod p$ and the values of e_1, e_2, p, and q are public, Eve can find the value of d using exhaustive search. Eve can now choose a message of her own M, calculates S_1 and S_2. Eve then sends M, S_1, and S_2 to Bob and pretends that they are coming from Alice.

23. In ElGamal scheme, if Eve can somehow finds out what value of r is used by Alice to calculate the signature for a particular message, the whole system is broken. Eve knows the value of M, S_1, S_2 and r. She can calculate the value of d as shown below:

$$\boldsymbol{d = (M - rS_2)S_1^{-1} \bmod (p - 1)}$$

This is possible if **gcd**$(S_1, p - 1) = 1$, which is very probable. When d is found, Eve can choose a message of her own (selective forgery), calculate the signature and send them to Bob fooling him that the message is coming from Alice.

25. In DSS scheme, if the value of r revealed, the whole system is broken. Eve knows the value of M, S_1, S_2 and r. She can calculate the value of d as shown below:

$$\boldsymbol{d = (rS_2 - h(M))S_1^{-1} \bmod q}$$

This is possible if **gcd**$(S_1, q) = 1$, which is very probable. When d is found, Eve can choose a message of her own (selective forgery), calculate the signature and send them to Bob fooling him that the message is coming from Alice.

27. This is done to make the calculation possible because if $a^x \equiv a^y \bmod p$, then $x \equiv y \bmod (p - 1)$.

29. In the DSS scheme, we need to make both S_1 and S_2 smaller than q. However, to make it more difficult for Eve to find the value of r, we first do exponentiation in modulo p (which is much larger than q), but we apply another modulo operation to reduce the size of S_1. In case of S_2, since there is no exponentiation and the size of the digest is smaller than q, we need to apply only a modulo q operation to make the size of S_2 smaller than q.

31. We start with V and show that it is congruent to S_1. Let h(M) = x.

$$V = (e_1^{xS_2^{-1}}\ e_2^{S_1\ S_2^{-1}} \bmod p \bmod q\ = (e_1^{x}\ \ e_2^{S_1})^{\ S_2^{-1}} \bmod p \bmod q$$

$$V = (e_1^{x}\ \ e_1^{dS_1})^{\ S_2^{-1}} \bmod p \bmod q \qquad \text{// Since } e_2 = e_1^{\mathrm{d}} \bmod p$$

$$V = (e_1^{x\,+\,dS_1})^{\ S_2^{-1}} \bmod p \bmod q$$

$$V = (e_1^{\ rS_2})^{\ S_2^{-1}} \bmod p \bmod q \qquad \text{// Since } S_2 = (x + dS)\ r^{-1} \bmod q$$

$$V = (e_1^{r})^{\ S_2S_2^{-1}} \bmod p \bmod q = (e_1^{r}) \bmod p \bmod q = S_1$$

33.

```
RSA_Signing (M, d, n)
{
        S ← $M^d$ mod n
        return (M, S)
}
```

```
RSA_Verifying (M, e, n, S)
{
        M′ ← $S^e$ mod n
        if (M’ = M)
                Accept M
        else
                Reject M
}
```

35.

```
**Schnorr_Signing** (M, $r$, $e_1$, $d$, $p$, $q$)
{
        $S_1 \leftarrow h(M \mid e_1^{r} \bmod p)$
        $S_2 \leftarrow (r + d \times S_1) \bmod q$
        return (M, $S_1$, $S_2$)
}
```

```
**Schnorr_Verifying** (M, $e_1$, $e_2$, $p$, $q$, $S_1$, $S_2$)
{
        $V \leftarrow h(M \mid e_1^{S_1} \times e_2^{-S_2} \bmod p)$
        if ($S_1 = V$)
                Accept M
        else
                Reject M
}
```

37.

```
**EllipticCurve_Signing** (M, $a$, $b$, $r$, $e_1(\ldots, \ldots)$, $d$, $p$, $q$)
{
        $P(u, v) \leftarrow r \times e_1(\ldots, \ldots)$
        $S_1 \leftarrow u \bmod q$
        $S_2 \leftarrow (h(M) + d \times S_1)\, r^{-1} \bmod q$
        return (M, $S_1$, $S_2$)
}
```

```
**EllipticCurve_Verifying** (M, $a$, $b$, $e_1(\ldots, \ldots)$, $e_1(\ldots, \ldots)$, $p$, $q$, $S_1$, $S_2$)
{
        $A \leftarrow (h(M) \times S_2^{-1}) \bmod q$
        $B \leftarrow (S_1 \times S_2^{-1}) \bmod q$
        $T(x, y) \leftarrow A \times e_1(\ldots, \ldots) + B \times e_1(\ldots, \ldots)$
        $V \leftarrow x \bmod q$
        if ($S_1 = V$)
                Accept M
        else
                Reject M
}
```