1 Question 8.6

Problem

Here is a variation of the *ElGamal Signature Scheme*. The key is constructed in a similar manner as before: Alice chooses $\alpha \in Z_p*$ to be a primitive element, $0 \leq a \leq p-2$ where $\gcd(a, p-1)= 1$, and $\beta = \alpha^a \ mod \ p$. The key $K = (\alpha, a, \beta)$, where α and β are the public key and a is the private key. Let $x \in Z_p$ be a message to be signed. Alice computes the signature $sig(x) = (\gamma, \delta)$, where

$$\gamma = \alpha^k \ mod \ p \tag{1}$$

and

$$\delta = (x - k\gamma)a^{-1} \ mod \ (p-1) \tag{2}$$

The only difference from the original *ElGamal Signature Scheme* is in the computation of δ. Answer the following questions concerning this modified scheme.

Part A

Describe how a signature (γ, δ) on a message x would be verified using Alice's public key.

Reordering δ:

$$\delta \equiv (x - k\gamma)a^{-1} \ mod \ (p-1)$$
$$a\delta \equiv (x - k\gamma) \ mod \ (p-1)$$
$$x \equiv (a\delta + k\gamma) \ mod \ (p-1)$$

Working backwards:

$$\alpha^x \equiv \alpha^{a\delta + k\gamma} \equiv \alpha^{a\delta}\alpha^{k\gamma} = (\alpha^a)^\delta(\alpha^k)^\gamma \equiv \beta^\delta\gamma^\gamma \ (mod \ p)$$

$$ver_K(x, (\gamma, \delta)) = true \iff \alpha^x \equiv \beta^\delta\gamma^\gamma \ (mod \ p)$$

Since α, β, and p are part of Alice's public key, we can prove that the message, x, is verified using the public key variables β and p and the signature variables δ and γ.

Part B

Describe a computational advantage of the modified scheme over the original scheme.

(I'm not completely sure on my answer here.)

In the original scheme, one would have to pick a k value that was invertible in $mod \ (p-1)$. In the modified scheme, we are inverting a, a primitive element, which is guaranteed to be invertible in $mod \ (p-1)$. It takes more cycles to find a k that is invertible than it does to just use a, which if chosen correctly does not need to be checked.

Part C

Briefly compare the security of the original and modified scheme.
The security of the modified scheme is less of that of the original scheme.

2 Question 8.7

Problem

Suppose Alice uses the DSA with $q = 101$, $p = 7879$, $\alpha = 170$, $a = 75$, and $\beta = 4567$, as in Example 8.4. Determine Alice's signature on a message x such that SHA3-224(x) = 52, using the random value $k = 49$, and show how the resulting signature is verified.

Solution

Table of known values below:

Variable	Value
q	101
p	7879
α	170
a	75
β	4567
$SHA3 - 224(x)$	52
k	49

Table 1: Table of known values

Finding γ:

$$\gamma = (\alpha^k \ mod \ p) \ mod \ q = (170^{49} \ mod \ 7879) \ mod \ 101 = 1776 \ mod \ 101 = 59 \tag{3}$$

Finding δ:

$$\delta = (SHA3 - 224(x) + a\gamma) * k^{-1} \ mod \ q = (52 + 75 * 59) * 49^{-1} \ mod \ 101 \tag{4}$$

$$\delta = 33 * (52 + 75 * 59) \ mod \ 101 = 79 \tag{5}$$

Signature:

$$sig_K(x, 49) = (59, 79) \tag{6}$$

Verification, finding e_1:

$$e_1 = SHA3 - 224(x) * \delta^{-1} \ mod \ q = 52 * 79^{-1} \ mod \ 101 = 52 * 78 \ mod \ 101 = 16 \tag{7}$$

Finding e_2:

$$e_2 = \gamma * \delta^{-1}\ mod\ q = 59 * 78\ mod\ 101 = 57 \tag{8}$$

Verification:

$$ver_K(x, (59, 79)) = true \iff (\alpha^{e_1} * \beta^{e_2}\ mod\ p)\ mod\ q = \gamma \tag{9}$$

$$(170^{16} * 4567^{57}\ mod\ 7879)\ mod\ 101 = 59 \tag{10}$$

$$1776\ mod\ 101 = 59 \tag{11}$$

$$59 = 59 \tag{12}$$

3 Question 8.10

Problem

Suppose that $x_0 \in 0, 1^*$ is a bitstring such that SHA3-224(x_0) = 00...0. Therefore, when used in DSA or $ECDSA$, we have that SHA3-224(x_0) $\equiv 0\ mod\ q$.

Part A

Show how it is possible to forge a DSA signature for the message x_0. HINT: Let $\delta = \gamma$, where γ is chosen appropriately.

The full DSA signature scheme is given below:

$$\gamma = (\alpha^{SHA3-224(x_0)*\delta^{-1}} * \beta^{\gamma\delta^{-1}}\ mod\ p)\ mod\ q$$

It's easy to see that if $SHA3 - 224(x) = 0$, then the above equation can reduce to:

$$\gamma = (\beta^{\gamma\delta^{-1}}\ mod\ p)\ mod\ q$$

Suppose again that we choose $\delta = \gamma$, then the follow occurs:

$$\gamma = (\beta^{\gamma\gamma^{-1}}\ mod\ p)\ mod\ q = (\beta\ mod\ p)\ mod\ q = \beta\ mod\ q$$

Given $SHA3 - 224(x_0) = 0$ and $\delta = \gamma$, we can forge signatures with the scheme below:

$$\gamma = \beta\ mod\ q$$

Since β is public from someone's signature, we can supply the following verification to utilize the scheme we derived above:

$$ver_K(x_0, (\beta, \beta))$$

Part B

Show how it is possible to forge an $ECDSA$ signature for the message x_0.

We can follow the same process from above for $ECDSA$ signatures. Suppose $SHA3-224(x) = 0$, then the verification scheme reduces to the following:

$$w = s^{-1} \ mod \ q$$

$$i = w * SHA3 - 224(x) \ mod \ q = w * 0 \ mod \ q = 0$$
$$j = wr \ mod \ q = s^{-1}r \ mod \ q$$
$$(u, v) = iA + jB = 0 * A + jB = jB$$
$$ver_K(x, (r, s)) = true \iff u \ mod \ q = r$$

Now suppose we set $r = s$, we can reduce the j variable to 1:

$$j = s^{-1}r \ mod \ q = s^{-1}s \ mod \ q = 1$$

Which we can then plug into our (u, v) equation:

$$(u, v) = 1 * B = B$$

Since B is public from the original signature scheme, we can take the x value from B and use it to verify the message, iff the hash of the message is 0:

$$ver_K(x, (B_x, B_x)) = true$$

4 Question 8.14

Problem

Let ε denote the elliptic curve $y^2 \equiv x^3 + x + 26 \ mod \ 127$. It can be shown that $\#\varepsilon = 131$, which is a prime number. Therefore any non-identity element in ε is a generator for $(\varepsilon, +)$. Suppose the $ECDSA$ is implemented in ε, with $A = (2, 6)$ and $m = 54$.

Part A

Compute the public key $B = mA$

$B = 54 * (2, 6) = (24, 44)$

Part B

Compute the signature on a message x if SHA3-224(x) $= 10$, when $k = 75$.

First we must compute kA, or $75 * (2, 6)$:

$$kA = (u, v) = 75 * (2, 6) = (88, 55) \tag{13}$$

Next, we can compute r:

$$r = 88 \ mod\ 131 = 88 \tag{14}$$

And now s:

$$s = 75^{-1}(10 + 54 * 88)\ mod\ 131 = 7 * (10 + 54 * 88)\ mod\ 131 = 60 \tag{15}$$

Our signature:

$$sig_K(x, 75) = (88, 60) \tag{16}$$

Part C

Show the computations used to verify the signature constructed in part (b).

First we compute w:

$$w = 60^{-1}\ mod\ 131 = 107 \tag{17}$$

Then we compute i:

$$i = 107 * 10\ mod\ 131 = 22 \tag{18}$$

Then we compute j:

$$j = 107 * 88\ mod\ 131 = 115 \tag{19}$$

Finally we compute (u, v):

$$(u, v) = 22 * (2, 6) + 15 * (24, 44) = (88, 55) \tag{20}$$

Our verification:

$$ver_K(x, (88, 60)) = true \iff 88\ mod\ 131 = 88 \tag{21}$$