Supplemental Problems for Problem Set #8

Due Friday, December 2, 2016

For this problem set, you'll need to use the following:

- Credential Set #1: $(p, \alpha, \beta) = (18743, 2, 801)$
- Credential Set #2: (p, q, α) are given in the *Mathematica* notebook nov16.nb on the course webpage
- Upload the *Mathematica* notebook that shows your work to onCourse. Make sure this is organized so that I can easily follow your work.
- Double-check that you have entered any quotes exactly as shown here!
  You'll want to be especially careful to check for spaces since sometimes things don't always look exactly the same when copying from a pdf.

Type I Problems

S-1. Which of the following are valid Elgamal digital signatures?
Use Credential Set #1.

(a) $(x, (r, s)) = (13432, (10220, 6280))$

(b) $(x, (r, s)) = (9723, (6008, 6499))$

(c) $(x, (r, s)) = (412, (618, 13718))$

S-2. Which of the following are valid DSA signatures?
Use Credential Set #2 with β equal to the following value

```
85726472212487237662673157019859316897933918089618701957 2
87413660211617718532302729494716165801144025989689985600 8
82756203703173437352943757403662037853388408244439013111 4
19137069285277501469064158437386559653818366239285111564 4
40657357464028517367455739923608379517708450990039320783 5
36637990944818141906058
```

Notice that this is NOT the β you get from using the d in the file nov16.nb.

(a) ("Gallia est omnis divisa in partes quattuor",
(1425257158900917706506592395533650161290 7,
960522914890659427223899441046750290382398415627))

(b) ("For all epsilon greater than zero, there exists a delta. . .",
(6329445958187022582843342856309529814579127020 3,
422664294359530587352509144018377716989536759486))

(c) ("So much time and so little to do. Wait a minute. Strike that. Reverse it.",
(2053872973416455397693511188380456683674189876 46,
101999815332226425266554734360331894486459243125 9))

Type II Problems

S-3. You observe the following two messages that Bob signed with Elgamal using Credential Set #1 and posted to Nik-Nak, a local Norton version of Yik-Yak.

("Peacock Pond is looking good today! No green fuzz!", (7036, 9026))
("Loving the new Kero Kero Bonito!!", (7036, 4230))

Bob did not sign the message x directly but instead signed the hash: SHA(x) mod p.

(a) Use this information to find Bob's private key d.

(b) You want to post the message

"If all pork chops were perfect, there wouldn't be hotdogs."

to Nik-Nak and make it look like it came from Bob.
You should use a different ephemeral key from the one Bob used in his first two messages, and generate Bob's Elgamal signature.
As above, you should sign SHA(x) mod p.

S-4. (a) Generate your own values for p and α to use with the Elgamal signature algorithm.
Your p should have at least 5 decimal digits, and demonstrate that α has the desirable properties for Elgamal signatures.
The *Mathematica* command Prime[n] gives you the nth prime number, which you might find handy.

(b) Determine your public credentials (p, α, β) to publish.

(c) Sign the message from S-3(b) using your Elgamal credentials.
As in that problem sign SHA(x) mod p.

S-5. (a) Use Credential Set #2 and generate your own β.
Determine your public DSA credentials to publish.

(b) Sign the message from S-3(b) using your DSA credentials.
Note that, unlike problems S-2 and S-3, you do not need to take the hash mod p since DSA has the hash built into the specifications.