ler Page

35

Received number: 35

Name: Gloire Rubambiza

Secret Number: 19

Calculated Number: 20 ✓

Shared Key: 14 ✓

Math 312, C. Wells **Thursday, April 12, 2018**

NAME: Gloire Rubambiza

each question on a new separate page and include your name and
:h page. For each additional page used, also indicate your name and

each page.

t all of the questions. Work on the ones that you feel ready for and

a calculator, your texts, and your notes.

: questions with your instructor for clarification.

- **Please indicate in table 1 which problems you wish to be evaluated.**

1	2	[✓ 3]	4	[✓ 5]	[✓ 6]	[✓ 7]	[✓ 8]
MC14	MC15	[✓ CS11]	CS9	[✓ CS10]	[✓ CS14]	[✓ CS15]	[✓ CS6]

Table 1: Questions and Learning Targets Addressed

Gloire Rubambiza
04/12/2018
MTH 312-01

In-Class Assessment 4

3) $g = 12, \quad p = 53$ ✓

$b = 19$

$B = 12^{19} \bmod 53 = 20$

$K = 35^{19} \bmod 53 = 14$

Gloire Rubambiza
04/12/2018
MTH 312-01

Assessment 4

5. a) $m = 14297$, $p = 33083$, $g = 186$, $B = 21866$

Nonce $(r) = 3$

$R = g^r = 186^3 = \boxed{6{,}434{,}856}$

$n = m \cdot B^r \bmod p = 14297 \cdot 21866^3 \bmod 33083$

$= \boxed{\cancel{1.494696262 \times 10^{17}}}$

Send n, R

5. b) $p = 33083$, $g = 186$, $b = 358$, $B = ?$

$B = g^b \bmod p$

$= 186^{358} \bmod 33083 = \boxed{1793}$ ✓

5. c) $p = 33083$, $g = 186$, $b = 358$, $C = 2509$, $R = 29433$

$\hookrightarrow n = 2509$

$c = n \cdot R^{p-1-b} \bmod p$

$= 2509 \cdot (29433)^{33083-1-358} \bmod 33083$

$= 2509\,(29433)^{32724} \bmod 33083$

$= 2509 \cdot 9867 \bmod 33083$

$\boxed{C = 10219}$ ✓

Gloire Rubambiza
04/12/2018
MTH 312-01

Assessment 4

6. $p = 66791$, $e = 3389$, $m = 10233$

$$n = m^{e} \bmod p$$

$$n = 10233^{3389} \bmod 66791$$

$$\boxed{n = 2238}$$ ✓

Gloire Rubambiza
04/12/2018
MTH 312-01

Assessment 4

7) The Pohlig-Hellman Cipher can be used to implement the three pass protocol by sharing a large prime (p) and each party choosing a secret exponent e. With the settings in place, Alice can encrypt a message m using $a = m^e \bmod p$ and send to Bob. Bob encrypts the message twice with his own secret exponent, and sends it back to Alice. Alice then removes her decryption and forwards to Bob who also decrypts the message to obtain Alice's original message (the shared key). Fermat's little theorem proves that the original message is recoverable.

What feature(s) of P-H make it a viable choice for 3pass?

Gloire Rubambiza
04/12/2018
MTH 312-01

Assessment 4

8.a) message "SEND HELP PLS"

encrypted: O1PJ T1AK KAO ✓

b) message: 6QPHA17HUO

decrypted: FINALEXAMS ✓