Solutions to HW08 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW08, Problem 2a, 2b

Zelda is going to do RSA with both Alice and Bob.
a) To set up RSA, Zelda sends Alice $(55, 33)$. Find d.

HW08, Problem 2a, 2b

Zelda is going to do RSA with both Alice and Bob.
a) To set up RSA, Zelda sends Alice $(55, 33)$. Find d.

SOLUTION

$N = 5 \times 11$, so $R = 4 \times 10 = 40$. Need $33^{-1} \pmod{40}$.
Wolfram alpha tells me $33^{-1} \pmod{40} = 17$.

HW08, Problem 2a, 2b

Zelda is going to do RSA with both Alice and Bob.
a) To set up RSA, Zelda sends Alice $(55, 33)$. Find d.
SOLUTION
$N = 5 \times 11$, so $R = 4 \times 10 = 40$. Need $33^{-1} \pmod{40}$.
Wolfram alpha tells me $33^{-1} \pmod{40} = 17$.

b) To set up RSA, Zelda sends Bob $(55, 23)$. Find d.

HW08, Problem 2a, 2b

Zelda is going to do RSA with both Alice and Bob.
a) To set up RSA, Zelda sends Alice $(55, 33)$. Find d.
SOLUTION
$N = 5 \times 11$, so $R = 4 \times 10 = 40$. Need $33^{-1} \pmod{40}$.
Wolfram alpha tells me $33^{-1} \pmod{40} = 17$.

b) To set up RSA, Zelda sends Bob $(55, 23)$. Find d.
SOLUTION
$N = 5 \times 11$, so $R = 4 \times 10 = 40$. Need $23^{-1} \pmod{40}$.
Wolfram alpha tells me $23^{-1} \pmod{40} = 7$.

HW08, Problem 2c, 2d

c) Alice sends Zelda 13. Whats the message? Show Work.

HW08, Problem 2c, 2d

c) Alice sends Zelda 13. Whats the message? Show Work.
SOLUTION Alice sends 13. Note that
$13^2 \equiv 169 \equiv 169 - 165 \equiv 4 \pmod{55}$. Zelda does

$$13^d \equiv 13^{17} \equiv 13 \times ((13)^2)^8 \equiv 13 \times 4^8 \equiv 18 \pmod{55}$$

HW08, Problem 2c, 2d

c) Alice sends Zelda 13. Whats the message? Show Work.
SOLUTION Alice sends 13. Note that
$13^2 \equiv 169 \equiv 169 - 165 \equiv 4 \pmod{55}$. Zelda does

$$13^d \equiv 13^{17} \equiv 13 \times ((13)^2)^8 \equiv 13 \times 4^8 \equiv 18 \pmod{55}$$

d) Bob sends Zelda 2. Whats the message? Show Work.

HW08, Problem 2c, 2d

c) Alice sends Zelda 13. Whats the message? Show Work.
SOLUTION Alice sends 13. Note that
$13^2 \equiv 169 \equiv 169 - 165 \equiv 4 \pmod{55}$. Zelda does

$$13^d \equiv 13^{17} \equiv 13 \times ((13)^2)^8 \equiv 13 \times 4^8 \equiv 18 \pmod{55}$$

d) Bob sends Zelda 2. Whats the message? Show Work.
SOLUTION Bob sends 2. Zelda does

$$2^d \equiv 2^7 \equiv 128 \equiv 128 - 110 \equiv 18 \pmod{55}$$

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

$$1 = 7 \times 33 - 10 \times 23.$$

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

$$1 = 7 \times 33 - 10 \times 23.$$

Eve knows $13 \equiv m^{33}$ and $2 \equiv m^{23}$.

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

$$1 = 7 \times 33 - 10 \times 23.$$

Eve knows $13 \equiv m^{33}$ and $2 \equiv m^{23}$.
Eve wants $(m^{33})^7 \times (m^{23})^{-10} \equiv m^{33\times 7-10\times 23} \equiv m^1$.

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

$$1 = 7 \times 33 - 10 \times 23.$$

Eve knows $13 \equiv m^{33}$ and $2 \equiv m^{23}$.
Eve wants $(m^{33})^7 \times (m^{23})^{-10} \equiv m^{33\times 7 - 10\times 23} \equiv m^1$.

$$(m^{33})^7 \times (m^{23})^{-10} \equiv 13^7 \times 2^{-10} = 13^7 \times (2^{-1})^{10}.$$

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

$$1 = 7 \times 33 - 10 \times 23.$$

Eve knows $13 \equiv m^{33}$ and $2 \equiv m^{23}$.
Eve wants $(m^{33})^7 \times (m^{23})^{-10} \equiv m^{33\times 7 - 10\times 23} \equiv m^1$.

$$(m^{33})^7 \times (m^{23})^{-10} \equiv 13^7 \times 2^{-10} = 13^7 \times (2^{-1})^{10}.$$

Need $2^{-1} \pmod{55}$, which is 28. SO we have

HW08, Problem 2e

e) Use the Same-N attack to recover the msg. Show work.
SOLUTION All $\equiv$ are mod 55.
$33, 23$ rel prime. 1 as a linear comb of 23 and 33:

$$1 = 7 \times 33 - 10 \times 23.$$

Eve knows $13 \equiv m^{33}$ and $2 \equiv m^{23}$.
Eve wants $(m^{33})^7 \times (m^{23})^{-10} \equiv m^{33\times 7-10\times 23} \equiv m^1$.

$$(m^{33})^7 \times (m^{23})^{-10} \equiv 13^7 \times 2^{-10} = 13^7 \times (2^{-1})^{10}.$$

Need $2^{-1} \pmod{55}$, which is 28. SO we have

$$13^7 \times 28^{10} \equiv 7 \times 34 \equiv 18$$

HW08, Problem 3

A triple N_1, N_2, N_3 is **pairwise rel prime** if N_1, N_2 are rel prime AND N_1, N_3 are rel prime AND N_2, N_3 are rel prime. Note N_1 is rel prime to $N_2 N_3$. Prove the following (its the CRT for $L = 3$).

HW08, Problem 3

A triple N_1, N_2, N_3 is **pairwise rel prime** if N_1, N_2 are rel prime AND N_1, N_3 are rel prime AND N_2, N_3 are rel prime. Note N_1 is rel prime to $N_2 N_3$. Prove the following (its the CRT for $L = 3$).

$a, b, c, N_1, N_2, N_3 \in \mathbb{N}$ **such that** N_1, N_2, N_3 **are pairwise relprime. Then** $\exists 0 \le x \le N_1 N_2 N_3$ **such that:**

$x \equiv a \pmod{N_1} \qquad x \equiv b \pmod{N_2} \qquad x \equiv c \pmod{N_3}$.

(You may use that if d, e are rel prime then $d^{-1} \pmod{e}$ exists.)

HW08, Problem 3

A triple N_1, N_2, N_3 is **pairwise rel prime** if N_1, N_2 are rel prime AND N_1, N_3 are rel prime AND N_2, N_3 are rel prime. Note N_1 is rel prime to N_2N_3. Prove the following (its the CRT for $L = 3$).
$a, b, c, N_1, N_2, N_3 \in \mathbb{N}$ **such that** N_1, N_2, N_3 **are pairwise relprime. Then** $\exists 0 \le x \le N_1N_2N_3$ **such that:**
$x \equiv a \pmod{N_1} \qquad x \equiv b \pmod{N_2} \qquad x \equiv c \pmod{N_3}$.
(You may use that if d, e are rel prime then $d^{-1} \pmod{e}$ exists.)

SOLUTION

$N_{12}^{-1} = (N_1N_2)^{-1} \pmod{N_3} \qquad N_{13}^{-1} = (N_1N_3)^{-1} \pmod{N_2}$
$N_{23}^{-1} = (N_2N_3)^{-1} \pmod{N_1}$,

$$y = aN_2N_3N_{23}^{-1} + bN_1N_3N_{13}^{-1} + cN_1N_2N_{12}^{-1}$$

Note that
$y \pmod{N_1} = a$
$y \pmod{N_2} = b$
$y \pmod{N_3} = c$
But $N_1N_2N_3 < y$ which is bad. We take $x \equiv y \pmod{N_1N_2N_3}$.