# HW Review

October 21, 2019

# Hw 2, Problem 2

Klingons-alphabet-35, Vulcans–36, Romulans–37.

1. Why is it easier for Vulcans to use PLAYFAIR than Klingons or Romulans?

# Hw 2, Problem 2

Klingons-alphabet-35, Vulcans–36, Romulans–37.

1. Why is it easier for Vulcans to use PLAYFAIR than Klingons or Romulans?
   **ANSWER** Vulcans: 36 is a square, so they do not need to fiddle with the letters. CAVEAT Klingons COULD arrange letters in $5 \times 7$ grid. Romulans are out-of-luck.

# Hw 2, Problem 2

Klingons-alphabet-35, Vulcans–36, Romulans–37.

1. Why is it easier for Vulcans to use PLAYFAIR than Klingons or Romulans?
   **ANSWER** Vulcans: 36 is a square, so they do not need to fiddle with the letters. CAVEAT Klingons COULD arrange letters in $5 \times 7$ grid. Romulans are out-of-luck.
2. How can Klingons use Playfair?

# Hw 2, Problem 2

Klingons-alphabet-35, Vulcans–36, Romulans–37.

1. Why is it easier for Vulcans to use PLAYFAIR than Klingons or Romulans?
   **ANSWER** Vulcans: 36 is a square, so they do not need to fiddle with the letters. CAVEAT Klingons COULD arrange letters in $5 \times 7$ grid. Romulans are out-of-luck.
2. How can Klingons use Playfair?
   **ANSWER** Klingons need to add one dummy character to their alphabet so it has 36, a square. CAVEAT See above.

# Hw 2, Problem 2

Klingons-alphabet-35, Vulcans–36, Romulans–37.

1. Why is it easier for Vulcans to use PLAYFAIR than Klingons or Romulans?
   **ANSWER** Vulcans: 36 is a square, so they do not need to fiddle with the letters. CAVEAT Klingons COULD arrange letters in $5 \times 7$ grid. Romulans are out-of-luck.
2. How can Klingons use Playfair?
   **ANSWER** Klingons need to add one dummy character to their alphabet so it has 36, a square. CAVEAT See above.
3. How can Romulans use Playfair?

# Hw 2, Problem 2

Klingons-alphabet-35, Vulcans–36, Romulans–37.

1. Why is it easier for Vulcans to use PLAYFAIR than Klingons or Romulans?
   **ANSWER** Vulcans: 36 is a square, so they do not need to fiddle with the letters. CAVEAT Klingons COULD arrange letters in $5 \times 7$ grid. Romulans are out-of-luck.
2. How can Klingons use Playfair?
   **ANSWER** Klingons need to add one dummy character to their alphabet so it has 36, a square. CAVEAT See above.
3. How can Romulans use Playfair?
   **ANSWER** Romulans select 2 characters to merge into 1, perhaps the 2 least used. so that their alphabet will have 36. CAVEAT Could add one and use $2 \times 19$ grid. Bad idea?

# Hw 3, Problem 2a

Alice wants to compute $7^{81} \pmod{101}$. Do this using repeated squaring. Show all work. How many multiplications does it take?

# Hw 3, Problem 2a

Alice wants to compute $7^{81} \pmod{101}$. Do this using repeated squaring. Show all work. How many multiplications does it take?

**ANSWER** all arithmetic is mod 101.

$7^2 \equiv (7^1)^2 \equiv 49$

$7^4 \equiv (7^2)^2 \equiv 49^2 \equiv 78$

$7^8 \equiv (7^4)^2 \equiv 78^2 \equiv 24$

$7^{16} \equiv (7^8)^2 \equiv 24^2 \equiv 71$

$7^{32} \equiv (7^{16})^2 \equiv 71^2 \equiv 92$

$7^{64} \equiv (7^{32})^2 \equiv 92^2 \equiv 81$

Each of the above took one mult for a total of 6 mults so far.

$7^{81} = 7^{64} \times 7^{16} \times 7^1 \equiv 81 \times 71 \times 7 \equiv 59$ (2 mults)

TOTAL: 8 mults.

# Hw 3, Problem 2b

Alice notices that $81 = 3^4$. So instead of using repeated *squaring* she decides to use repeated *cubing*. Each cubing takes two multiplications but there are less iterations. Compute $7^{81}$ using this, show your work. How many multiplications does it take?

# Hw 3, Problem 2b

Alice notices that $81 = 3^4$. So instead of using repeated *squaring* she decides to use repeated *cubing*. Each cubing takes two multiplications but there are less iterations. Compute $7^{81}$ using this, show your work. How many multiplications does it take?

**ANSWER** All arith is mod 101.

$7^3 \equiv 40$

$7^9 \equiv (7^3)^3 \equiv 40^3 \equiv 67$

$7^{27} \equiv (7^9)^3 \equiv 67^3 \equiv 86$

$7^{81} \equiv (7^{27})^3 = 86^3 \equiv 59$

Each of the above took two mult for a total of 8 mults.

TOTAL: 8 mults.

# Hw 3, Problem 2c

Give algorithm for repeated cubing method for: given $a, n, p$, find $a^n \pmod{p}$. Give upper bound on numb. of mults as function $n$.

# Hw 3, Problem 2c

Give algorithm for repeated cubing method for: given $a, n, p$, find $a^n \pmod p$. Give upper bound on numb. of mults as function $n$.

**ANSWER**

All arithmetic is mod $p$.

1. Input $(a, n, p)$
2. $n = (n_L \cdots n_0)_3$. $(n_i \in \{0, 1, 2\}$, $L = \lfloor \log_3(n) \rfloor$.)
3. $x_0 = a$
4. For $i = 1$ to $L$, $x_i = x_{i-1}^3$. (Note that $x_i = a^{3^i}$.)
5. (Now have $a^{n_0 3^0}, \ldots, a^{n_L 3^L}$) Answer is $a^{n_0 3^0} \times \cdots \times a^{n_L 3^L}$

$L$ iters, 2 mults per iter: $\leq 2L \leq 2 \lfloor \log_3(n) \rfloor \leq 2 \log_3(n)$ mults.
Mults after iterations, : $\leq L = \lfloor \log_3(n) \rfloor \leq \log_3(n)$.
Total: $\leq 3 \log_3(n)$ mults.

# Hw 3, Problem 2d

Repeated squaring: the number of multiplications is

$$\leq \lg(n) + (\text{ Number of 1's in binary rep of } n\ ) - 1.$$

Give three examples of an $n \geq 99$ where the repeated-cubing algorithm takes less mults than the repeated-squaring algorithm.

# Hw 3, Problem 2d- Cubing

# Hw 3, Problem 2d- Cubing

**ANSWER**

We look at powers of 3. $7^{3^5}$. First do by repeated cubing:

$x_0 = 7$

$x_1 \equiv x_0^3$ (which is $7^3$)

$x_2 \equiv x_1^3$ (which is $7^{3^2}$)

$x_3 \equiv x_2^3$ (which is $7^{3^3}$)

$x_4 \equiv x_3^3$ (which is $7^{3^4}$)

$x_5 \equiv x_4^3$ (which is $7^{3^5}$)

Each line takes 2 mults, so 10 mults total.

# Hw 3, Problem 2d- Squaring

We now look at repeated squares.

Need to look at $3^5$ in binary: $3^5 = 243 = 11110011$ in binary.

$$11110011 = 2^7 + 2^6 + 2^5 + 2^4 + 2^1 + 2^0$$

# Hw 3, Problem 2d- Squaring

We now look at repeated squares.

Need to look at $3^5$ in binary: $3^5 = 243 = 11110011$ in binary.

$$11110011 = 2^7 + 2^6 + 2^5 + 2^4 + 2^1 + 2^0$$

$x_0 = 7$

$x_1 \equiv x_0^2$ (which is $7^2$)

$x_2 \equiv x_1^2$ (which is $7^{2^2}$)

$x_3 \equiv x_2^2$ (which is $7^{2^3}$)

$x_4 \equiv x_3^2$ (which is $7^{2^4}$)

$x_5 \equiv x_4^2$ (which is $7^{2^5}$)

$x_6 \equiv x_5^2$ (which is $7^{2^6}$)

$x_7 \equiv x_6^2$ (which is $7^{2^7}$)

7 multiplications so far.

# Hw 3, Problem 2d- Squaring

We now look at repeated squares.

Need to look at $3^5$ in binary: $3^5 = 243 = 11110011$ in binary.

$$11110011 = 2^7 + 2^6 + 2^5 + 2^4 + 2^1 + 2^0$$

$x_0 = 7$

$x_1 \equiv x_0^2$ (which is $7^2$)

$x_2 \equiv x_1^2$ (which is $7^{2^2}$)

$x_3 \equiv x_2^2$ (which is $7^{2^3}$)

$x_4 \equiv x_3^2$ (which is $7^{2^4}$)

$x_5 \equiv x_4^2$ (which is $7^{2^5}$)

$x_6 \equiv x_5^2$ (which is $7^{2^6}$)

$x_7 \equiv x_6^2$ (which is $7^{2^7}$)

7 multiplications so far. And now we do:

$$7^{3^5} = 7^{2^0} \times 7^{2^1} \times 7^{2^4} \times 7^{2^5} \times 7^{2^6} \times 7^{2^7}$$

This is 5 mults. Total Number of mults: 12, more than 10.

We OMIT the other two examples, but they are both powers of 3.

# Hw 3, Problem 2e

Why isn't repeated cubing used more often?

# Hw 3, Problem 2e

Why isn't repeated cubing used more often?

**ANSWER**

- Sometimes it takes more steps.

# Hw 3, Problem 2e

Why isn't repeated cubing used more often?

**ANSWER**

- Sometimes it takes more steps.
- But even when it takes less, multiplying by powers of 2 is a very easy shift of bits, so the type of mult is easier for powers of 2.

# Hw 3, Problem 3

Alice and Bob are going to use the Affine Cipher. They get to choose their alphabet size! If the alphabet size is $n$ then they will pick a number $a \in \{1, \ldots, n\}$ at *random* and then test if $a$ will work to be the coefficient of $x$. If not, then try again. If so then they will use $a$ as the coefficient for $x$. (We are not concerned with the picking of $b$.)

# Hw 3, Problem 3a

Assume the alphabet size is 1000. What is the probability that the $a$ they pick will work? Call this $p_{1000}$. (Think about but do not hand in: what is the expected number of times they will need to pick an $a$?)

# Hw 3, Problem 3a

Assume the alphabet size is 1000. What is the probability that the $a$ they pick will work? Call this $p_{1000}$. (Think about but do not hand in: what is the expected number of times they will need to pick an $a$?)

**ANSWER** We need to know how many elements of $\{1, \ldots, 1000\}$ are rel prime to 1000.

# Hw 3, Problem 3a

Assume the alphabet size is 1000. What is the probability that the $a$ they pick will work? Call this $p_{1000}$. (Think about but do not hand in: what is the expected number of times they will need to pick an $a$?)

**ANSWER** We need to know how many elements of $\{1, \ldots, 1000\}$ are rel prime to 1000. This is

$$\phi(1000) = \phi(2^3 \times 5^3) = \phi(2^3) \times \phi(5^3) =$$

$$= (2^3 - 2^2)(5^3 - 5^2) = 4 \times 100 = 400$$

# Hw 3, Problem 3a

Assume the alphabet size is 1000. What is the probability that the $a$ they pick will work? Call this $p_{1000}$. (Think about but do not hand in: what is the expected number of times they will need to pick an $a$?)

**ANSWER** We need to know how many elements of $\{1, \ldots, 1000\}$ are rel prime to 1000. This is

$$\phi(1000) = \phi(2^3 \times 5^3) = \phi(2^3) \times \phi(5^3) =$$

$$= (2^3 - 2^2)(5^3 - 5^2) = 4 \times 100 = 400$$

Hence the probability that a random chosen numbers is rel prime to 1000 is

$$p_{1000} = \frac{400}{1000} = 0.4.$$

# Hw 3, Problem 3a, the THINK ABOUT part

Think about but do not hand in: what is the expected number of times they will need to pick an $a$?

# Hw 3, Problem 3a, the THINK ABOUT part

Think about but do not hand in: what is the expected number of times they will need to pick an $a$?

What is the expected number of times they will need to pick an $a$?

$$\sum_{i=1}^{\infty} (\text{Prob that takes } i \text{ tries}) \times i$$

# Hw 3, Problem 3a, the THINK ABOUT part

Think about but do not hand in: what is the expected number of times they will need to pick an $a$?

What is the expected number of times they will need to pick an $a$?

$$\sum_{i=1}^{\infty} (\text{Prob that takes } i \text{ tries}) \times i$$

The prob it takes $i$ tries is
(Prob the first $i-1$ tries don't work)$\times$(Prob the $i$th try does work)

$$= (1-0.4)^{i-1} \times 0.4 = (0.6)^{i-1}(0.4)$$

# Hw 3, Problem 3a, the THINK ABOUT part

Think about but do not hand in: what is the expected number of times they will need to pick an $a$?

What is the expected number of times they will need to pick an $a$?

$$\sum_{i=1}^{\infty} (\text{Prob that takes } i \text{ tries}) \times i$$

The prob it takes $i$ tries is
(Prob the first $i-1$ tries don't work)$\times$(Prob the $i$th try does work)

$$= (1-0.4)^{i-1} \times 0.4 = (0.6)^{i-1}(0.4)$$

So answer is

$$\sum_{i=1}^{\infty} (0.6)^{i-1} \times 0.4 \times i = (0.4) \sum_{i=1}^{\infty} (0.6)^{i-1} i =$$

# Hw 3, Problem 3a, the THINK ABOUT part

Think about but do not hand in: what is the expected number of times they will need to pick an $a$?

What is the expected number of times they will need to pick an $a$?

$$\sum_{i=1}^{\infty} (\text{Prob that takes } i \text{ tries}) \times i$$

The prob it takes $i$ tries is
(Prob the first $i-1$ tries don't work)$\times$(Prob the $i$th try does work)

$$= (1-0.4)^{i-1} \times 0.4 = (0.6)^{i-1}(0.4)$$

So answer is

$$\sum_{i=1}^{\infty} (0.6)^{i-1} \times 0.4 \times i = (0.4) \sum_{i=1}^{\infty} (0.6)^{i-1} i =$$

How to evaluate this sum?

# Hw3, Problem 3a- The Weird Sum

$$\sum_{i=1}^{\infty}(0.6)^{i-1}i =$$

Lets generalize this: $\sum_{i=1}^{\infty} ix^{i-1} =$
Does this remind you of anything?

# Hw3, Problem 3a- The Weird Sum

$$\sum_{i=1}^{\infty}(0.6)^{i-1}i =$$

Lets generalize this: $\sum_{i=1}^{\infty} ix^{i-1} =$
Does this remind you of anything? $\frac{d}{dx}x^i = ix^{i-1}$.

# Hw3, Problem 3a- The Weird Sum

$$\sum_{i=1}^{\infty}(0.6)^{i-1}i =$$

Lets generalize this: $\sum_{i=1}^{\infty} ix^{i-1} =$
Does this remind you of anything? $\frac{d}{dx}x^i = ix^{i-1}$.

$$\sum_{i=1}^{\infty} x^i = \frac{x}{1-x}$$

# Hw3, Problem 3a- The Weird Sum

$$\sum_{i=1}^{\infty}(0.6)^{i-1}i =$$

Lets generalize this: $\sum_{i=1}^{\infty} ix^{i-1} =$
Does this remind you of anything? $\frac{d}{dx}x^i = ix^{i-1}$.

$$\sum_{i=1}^{\infty} x^i = \frac{x}{1-x}$$

Differentiate both sides:

$$\sum_{i=1}^{\infty} ix^{i-1} = \frac{(1-x)+x}{(1-x)^2} = \frac{1}{(1-x)^2}$$

$$(0.4)\sum_{i=1}^{\infty} i(0.6)x^{i-1} = \frac{2}{5}\frac{1}{(2/5)^2} = 2.5$$

# Hw3, Problem 3a- The Weird Sum

$$\sum_{i=1}^{\infty}(0.6)^{i-1}i =$$

Lets generalize this: $\sum_{i=1}^{\infty} ix^{i-1} =$
Does this remind you of anything? $\frac{d}{dx}x^i = ix^{i-1}$.

$$\sum_{i=1}^{\infty} x^i = \frac{x}{1-x}$$

Differentiate both sides:

$$\sum_{i=1}^{\infty} ix^{i-1} = \frac{(1-x)+x}{(1-x)^2} = \frac{1}{(1-x)^2}$$

$$(0.4)\sum_{i=1}^{\infty} i(0.6)x^{i-1} = \frac{2}{5}\frac{1}{(2/5)^2} = 2.5$$

SO, not that many tries to get the proper $a$.

# HW 03, Problem 3b

Assume the alphabet size is 1001. What is the probability that the $a$ they pick will work?

# HW 03, Problem 3b

Assume the alphabet size is 1001. What is the probability that the $a$ they pick will work?

**ANSWER** We need to know how many elements of $\{1, \ldots, 1001\}$ are rel prime to 1001. This is

$$\phi(1001) = \phi(7 \times 11 \times 13) = \phi(7) \times \phi(11) \times \phi(13) = 6 \times 10 \times 12.$$

# HW 03, Problem 3b

Assume the alphabet size is 1001. What is the probability that the $a$ they pick will work?

**ANSWER** We need to know how many elements of $\{1, \ldots, 1001\}$ are rel prime to 1001. This is

$$\phi(1001) = \phi(7 \times 11 \times 13) = \phi(7) \times \phi(11) \times \phi(13) = 6 \times 10 \times 12.$$

Hence the probability is

$$p_{1001} = \frac{6 \times 10 \times 12}{1001} = \frac{720}{1001} \sim 0.72.$$

# HW 03, Problem 3c

Which of $p_{1000}$ and $p_{1001}$ is bigger? Based on this give some general advice on what alphabet size to use if a prime size is not available.

# HW 03, Problem 3c

Which of $p_{1000}$ and $p_{1001}$ is bigger? Based on this give some general advice on what alphabet size to use if a prime size is not available.

**ANSWER** $p_{1001}$ is bigger.

# HW 03, Problem 3c

Which of $p_{1000}$ and $p_{1001}$ is bigger? Based on this give some general advice on what alphabet size to use if a prime size is not available.

**ANSWER** $p_{1001}$ is bigger.
Good to pick an alphabet size that has no square factors.

# HW 03, Problem 5

Alice and Bob are using the cipher on the Sept 9 slides, title *Awesome Vig or Psuedo One-Time Pad* EXCEPT that the mod is 2 digits long instead of 4 digits long.
Eve is sure that the word ERIK will be in the plaintext.
Eve looks at every 4-long sequence in the ciphertext and guesses that they decode to ERIK and sets up equations.
Eve sees ABCD.

# HW 03, Problem 5

Alice and Bob are using the cipher on the Sept 9 slides, title *Awesome Vig or Psuedo One-Time Pad* EXCEPT that the mod is 2 digits long instead of 4 digits long.
Eve is sure that the word ERIK will be in the plaintext.
Eve looks at every 4-long sequence in the ciphertext and guesses that they decode to ERIK and sets up equations.
Eve sees ABCD.

The following table will help you:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

# HW 03, Problem 5a

Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

# HW 03, Problem 5a

Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

ERIK is (05,18,09,11). ABCD is (01,02,03,04) Here is how Eve finds her guess for this part of the key:

# HW 03, Problem 5a

Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

ERIK is (05,18,09,11). ABCD is (01,02,03,04) Here is how Eve finds her guess for this part of the key:
The first two digits:
$0 + x \equiv 0 \mod 10$
$5 + y \equiv 1 \pmod{10}$

# HW 03, Problem 5a

Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

ERIK is (05,18,09,11). ABCD is (01,02,03,04) Here is how Eve finds her guess for this part of the key:
The first two digits:
$0 + x \equiv 0 \mod 10$
$5 + y \equiv 1 \pmod{10}$
Hence $x = 0$ and $y = 6$.
Keep doing this to find that the guess for the key for this part is $(06, 94, 04, 93)$

# HW 03, Problem 5a

Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

ERIK is (05,18,09,11). ABCD is (01,02,03,04) Here is how Eve finds her guess for this part of the key:
The first two digits:
$0 + x \equiv 0 \mod 10$
$5 + y \equiv 1 \pmod{10}$
Hence $x = 0$ and $y = 6$.
Keep doing this to find that the guess for the key for this part is $(06, 94, 04, 93)$
Just for my own sanity I'll rewrite this to check it.

| | | | | |
|---|---|---|---|---|
| ERIK | 05 | 18 | 09 | 11 |
| KEY | 06 | 94 | 04 | 93 |
| ABCD | 01 | 02 | 03 | 04 |

# HW 03, Problem 5a, Cont

The conjecture is that the key for this part is $(06, 94, 04, 93)$.
We need to test that.
RECALL that the the key is formed by a recurrence of the form

$$x_i = Ax_{i-1} + B \pmod{M}$$

So if the sequence $(06, 94, 04, 93)$ is part of the key then we must have:

$$\begin{aligned} 94 &\equiv 6A + B \pmod{M} \\ 4 &\equiv 94A + B \pmod{M} \\ 93 &\equiv 4A + B \pmod{M} \end{aligned}$$

# HW 03, Problem 5b

What are the bounds on $M$?

# HW 03, Problem 5b

What are the bounds on $M$?

**ANSWER** We know that $M$ is 2-digits long so $M \leq 99$.
We know that one of the numbers in the key is 94, so $95 \leq M$.
Hence

$$95 \leq M \leq 99$$

# HW 03, Problem 5c

Solve the equations or show they can't be solved:

$$\begin{aligned} 94 &\equiv 6A + B \pmod{M} \\ 4 &\equiv 94A + B \pmod{M} \\ 93 &\equiv 4A + B \pmod{M} \end{aligned}$$

AND $95 \leq M \leq 99$. All $\equiv$ are mod $M$.
Subtract the second from the first equation to get EQ1 $90 \equiv -88A$
Subtract the third from the first equation to get EQ2 $1 \equiv 2A$
Multiply EQ2 by 44 to get EQ3 $44 \equiv 88A$
Add EQ1 and EQ3 to get $134 \equiv 0$. Hence $M$ divides 134.

So $M$ has to be one of $1, 2, 67, 134$.
NONE of these are between 95 to 99 so NO value of $M$ works.

# HW 04, Problem 2

Alice and Bob are going to use Diffie-Hellman. Bob wants to save some time so instead of picking a RANDOM $b \in \{\frac{p}{3}, \frac{2p}{3}\}$ he picks a $b$ that is a power of 2 because he thinks that for such $b$, $g^b$ will be easier to compute. (Alice still picks $a \in \{\frac{p}{3}, \frac{2p}{3}\}$ at random.)

# HW 04, Problem 2a

Bob is right! Computing $g^b$ IS easier if $b$ is a power of 2. Explain why.

# HW 04, Problem 2a

Bob is right! Computing $g^b$ IS easier if $b$ is a power of 2. Explain why.

**ANSWER**

Recall that repeated squaring for $g^b$ takes

$$\lfloor \log_2(b) \rfloor + \text{ (number of 1's in } b \text{ in binary)-1}$$

mults. But if $b$ is a power of 2 then there is only one 1 in $b$ in binary. So only $\lfloor \log_2(b) \rfloor$ mults.

# HW 04, Problem 2b

Eve can now find the shared secret in time $O(\log p)^c$. Show how. What is $c$?

# HW 04, Problem 2b

Eve can now find the shared secret in time $O(\log p)^c$. Show how. What is $c$?

**ANSWER**

Eve knows that $b \in X = \{2^0, 2^1, \ldots, 2^{\lfloor \log_2 p \rfloor}\}$.

$X$ IS A VERY SMALL SET!

Eve sees $p, g, g^a, g^b$.

Eve computes $g^x$ for all $x \in X$. Each of these takes $O(\log p)$ mults, and there are $O(\log p)$ elements of $X$, so thats $O(\log p)^2$ mults. For one of those $x$ you will see that $g^x = g^b$, so Eve finds out what $b$ is. Once Eve knows $b$, she computes $(g^a)^b = g^{ab}$, so she has the secret. This last step took another $O(\log p)$ mults, so still

$$O(\log p)^2 \text{ mults, so } c = 2.$$

One can be a bit cleverer and get $c = 1$.

# HW 04, Problem 2b, extra

We need to compute $g^x$ for every $x \in X$. But note that

$$X = \{2^0, 2^1, \ldots, 2^{\lfloor \log_2 p \rfloor}\}.$$

Hence we need

$g^{2^0}$

$g^{2^1}$

$g^{2^2}$

$\vdots$

$g^{2^{\lfloor \log_2 p \rfloor}}$

By repeated squaring an do this in $O(\log_2 p)$ steps.

# HW 05, Problem 6

Compute the following and show your work. (You may use a calculator for simple operations such as multiplication.)

1. (5 points) $7^{999,999,999,999,999} \pmod{100}$
2. (5 points) $7^{999,999,999,999,999} \pmod{101}$
3. (5 points) $7^{999,999,999,999,999} \pmod{102}$

# HW 05, Problem 6a

$$7^{999,999,999,999,999} \pmod{100}$$

# HW 05, Problem 6a

$7^{999,999,999,999,999} \pmod{100}$

**ANSWER** We need $\phi(100)$.

# HW 05, Problem 6a

$7^{999,999,999,999,999} \pmod{100}$

**ANSWER** We need $\phi(100)$.

$$\phi(100) = \phi(2^2 \times 5^2) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40$$

# HW 05, Problem 6a

$7^{999,999,999,999,999} \pmod{100}$

**ANSWER** We need $\phi(100)$.

$$\phi(100) = \phi(2^2 \times 5^2) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40$$

$$7^{999,999,999,999,999} \equiv 7^{999,999,999,999 \bmod 40} \pmod{100} \equiv 7^{39} \pmod{100}$$

# HW 05, Problem 6a, cont

Want $739 \pmod{100}$.
Need 39 as a sum of powers of 2. By taking the highest pow-of-2 that is $\leq$ current value:

$$39 = 2^5 + 2^2 + 2^1 + 2^0$$

All $\equiv$ are mod 100.

$7^0 \equiv 1$

$7^{2^0} \equiv 7$

$7^{2^1} \equiv (7^{2^0})^2 \equiv 7^2 \equiv 49$

$7^{2^2} \equiv (7^{2^1})^2 \equiv 49^2 \equiv 1$

$7^{2^3} \equiv (7^{2^2})^2 \equiv 1^2 \equiv 1$

$7^{2^4} \equiv (7^{2^3})^2 \equiv 1^2 \equiv 1$

$7^{2^5} \equiv (7^{2^4})^2 \equiv 1^2 \equiv 1$

$$7^{39} \equiv 7^{2^5} \times 7^{2^2} \times 7^{2^1} \times 7^{2^0} \equiv 1 \times 49 \times 7 \equiv 43$$

# HW 05, Problem 6a

$$7^{999,999,999,999,999} \pmod{101}$$

# HW 05, Problem 6a

$7^{999,999,999,999,999} \pmod{101}$

**ANSWER**

We need $\phi(101)$. This one is easy $\phi(101) = 100$.

$7^{999,999,999,999,999} \pmod{102}$

Use $\phi(102) = \phi(2 \times 3 \times 17) = 1 \times 2 \times 16 = 32$.

# HW 06, Problem 2a

Alice wants to speed up and simplify RSA. She tells Bob "lets ALWAYS use $e = 2^{2^4} + 1$". Let $e = 2^{2^4} + 1$ for the rest of this problem.

1) Write $e - 2, e - 1, e$ as both decimal and binary.

# HW 06, Problem 2a

Alice wants to speed up and simplify RSA. She tells Bob "lets ALWAYS use $e = 2^{2^4} + 1$". Let $e = 2^{2^4} + 1$ for the rest of this problem.

1) Write $e - 2, e - 1, e$ as both decimal and binary.

**ANSWER**

$e - 2 = 65535$ in base 10

$e - 2 = 1111111111111111$ in base 2.

$e - 1 = 65536$ in base 10

$e - 1 = 10000000000000000$ in base 2.

$e = 65537$ in base 10

$e = 10000000000000001$ in base 2.

# HW 06, Problems 2b

2b) Alice wants to speed up and simplify RSA.
If Bob computes $m^e$ using repeated squaring then how many operations will it take?
If Bob computes $m^{e-1}$ using repeated squaring then how many operations will it take?
If Bob computes $m^{e-2}$ using repeated squaring then how many operations will it take?

# HW 06, Problems 2b

2b) Alice wants to speed up and simplify RSA.
If Bob computes $m^e$ using repeated squaring then how many operations will it take?
If Bob computes $m^{e-1}$ using repeated squaring then how many operations will it take?
If Bob computes $m^{e-2}$ using repeated squaring then how many operations will it take?

**ANSWER**

Recall that repeated squaring for $m^n$ takes
$\lfloor \lg(n) \rfloor$ + (Number of 1's in $n$) $-1$.

$\lfloor \lg(e-2) \rfloor = 15$. Number of 1's in $e-2$ is 16. So 30 operations.
$\lfloor \lg(e-1) \rfloor = 16$. Number of 1's in $e-1$ is 1. So 16 operations.
$\lfloor \lg(e) \rfloor = 16$. Number of 1's in $e$ is 2. So 17 operations.

# HW 06, Problem 2c

2c) If you did part 2b right, then using $e-1$ is the best (though not by much), then $e$, then $e-2$ (and $e-2$ is much worse than $e$). So why not use $e-1$ for RSA?

# HW 06, Problem 2c

2c) If you did part 2b right, then using $e-1$ is the best (though not by much), then $e$, then $e-2$ (and $e-2$ is much worse than $e$). So why not use $e-1$ for RSA?

**ANSWER** $e-1$ would need to be rel prime to $(p-1)(q-1)$. But $(p-1)(q-1)$ is even since either $p$ or $q$ is odd. Hence, $e-1$ cannot work.

# HW 06, Problems 2d

2d) Give two PROS to using this value of $e$.

# HW 06, Problems 2d

2d) Give two PROS to using this value of $e$.
**ANSWER** I'll give three:
Computing $m^e$ takes only 17 operations (as seen above even a slight change might increase the number of operations by a lot).

This $e$ is known to be prime so easy to test if rel prime to $(p-1)(q-1)$.

$e$ is big enough to thwart attacks in 2019.

# HW 06, Problems 2e

2e) Give two CONS to using this value of $e$.

# HW 06, Problems 2e

2e) Give two CONS to using this value of $e$.

**ANSWER** I'll give three:

If keep using the SAME $e$ then Eve could prepossess stuff.

If keep using the SAME $e$ then — who knows — maybe number theorists will find out something special about that $e$ that makes it easy to find the inverse of mod $(p-1)(q-1)$.

This $e$ thwarts the low-$e$ attack TODAY, but what about Tomorrow, tomorrow, is always another day!

What if you have a company that has over $2^{2^4}+1$ customers? Then a low-$e$ attack WILL work.

# HW 06, Problem 2f

Do people really use this value of $e$? Is using this value of $e$ a good idea?

# HW 06, Problem 2f

Do people really use this value of $e$? Is using this value of $e$ a good idea?

**ANSWER** People really do use it. This makes me nervous.

# HW 06, Origin of Problem 2, and a Point

In Fall 2018 I had the following conversation with a student who I will call Ben since (1) he as a practical person like Ben in current class, and (2) his name really was Ben.

Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq gets a PhD on that value of $e$.

# HW 06, Origin of Problem 2, and a Point

In Fall 2018 I had the following conversation with a student who I will call Ben since (1) he as a practical person like Ben in current class, and (2) his name really was Ben.

Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq gets a PhD on that value of $e$.

Ben: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

# HW 06, Origin of Problem 2, and a Point

In Fall 2018 I had the following conversation with a student who I will call Ben since (1) he as a practical person like Ben in current class, and (2) his name really was Ben.

Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq gets a PhD on that value of $e$.

Ben: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a much better theorist than me. Email me the website and paper and I'll see whats up.

# HW 06, Origin of Problem 2, and a Point

In Fall 2018 I had the following conversation with a student who I will call Ben since (1) he as a practical person like Ben in current class, and (2) his name really was Ben.

Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq gets a PhD on that value of $e$.

Ben: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a much better theorist than me. Email me the website and paper and I'll see whats up.

Well pierce my ears and call me drafty! In practice you SHOULD use $e = 2^{2^4} + 1$.

# Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.

Bill: Can do $m^e$ with repeated squaring in roughly $\lg_2(m)$ steps.

Ben: roughly $\lg_2(m)$ steps? What does roughly mean?

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4-1}}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.

# Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.

Bill: Can do $m^e$ with repeated squaring in roughly $\lg_2(m)$ steps.

Ben: roughly $\lg_2(m)$ steps? What does roughly mean?

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}-1}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.

Bill: Does 16 vs 30 steps matter?

# Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.

Bill: Can do $m^e$ with repeated squaring in roughly $\lg_2(m)$ steps.

Ben: roughly $\lg_2(m)$ steps? What does roughly mean?

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}-1}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.

Bill: Does 16 vs 30 steps matter?

Ben: Yes you moron.

# Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.

Bill: Can do $m^e$ with repeated squaring in roughly $\lg_2(m)$ steps.

Ben: roughly $\lg_2(m)$ steps? What does roughly mean?

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}-1}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.

Bill: Does 16 vs 30 steps matter?

Ben: Yes you moron.

Bill: Only Justin is allowed to call me a moron.

# $e = 2^{2^4} + 1$ vs my fears

In Practice: Want to use $e = 2^{2^4} + 1$ since:

1. Only 15 mults.
2. $2^{2^4} + 1$ is big enough to ward off the low-e attacks
3. $2^{2^4} + 1$ is prime, so only way it fails to be rel prime to $R = (p-1)(q-1)$. is if it divides $R$. Unlikely and easily tested.

In Theory: Do not want to use the same $e$ over and over again for fear of this being exploited.

Who is Right: $e = 2^{16} + 1$ is right.

# $e = 2^{2^4} + 1$ vs my fears

In Practice: Want to use $e = 2^{2^4} + 1$ since:

1. Only 15 mults.
2. $2^{2^4} + 1$ is big enough to ward off the low-e attacks
3. $2^{2^4} + 1$ is prime, so only way it fails to be rel prime to $R = (p-1)(q-1)$. is if it divides $R$. Unlikely and easily tested.

In Theory: Do not want to use the same $e$ over and over again for fear of this being exploited.

Who is Right: $e = 2^{16} + 1$ is right. For now

# HW 06, Problem 3a

1) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

# HW 06, Problem 3a

1) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

**ANSWER**

$1001 = 7 \times 11 \times 13$. Hence

# HW 06, Problem 3a

1) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

**ANSWER**

$1001 = 7 \times 11 \times 13$. Hence

$\phi(1001) = 6 \times 10 \times 12 = 720$

# HW 06, Problem 3a

1) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

**ANSWER**

$1001 = 7 \times 11 \times 13$. Hence

$\phi(1001) = 6 \times 10 \times 12 = 720$

We need to compute

$123, 456, 789, 111, 213, 141 \pmod{720}$ which is 501

# HW 06, Problem 3a

1) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

**ANSWER**

$1001 = 7 \times 11 \times 13$. Hence

$\phi(1001) = 6 \times 10 \times 12 = 720$

We need to compute

$123, 456, 789, 111, 213, 141 \pmod{720}$ which is 501

So we just need

$$30^{501} \pmod{1001}$$

We omit the rest but it's done by repeated squaring.

# HW 6, Problem 3b

Give an algorithm that does the following: Given primes $p, q$ and $1 \leq a \leq pq - 1$ such that $a$ is rel prime to $pq$, and $n$, return $a^n \pmod{pq}$.

Any op with numbers less than $pq$ takes 1 step; any op with a number BIGGER than $pq$, of length $L$, takes $L$ steps. Give an upper bound on the number of ops in terms of $n, p, q$. Can use $O$-notation.

# HW 6, Problem 3b

Give an algorithm that does the following: Given primes $p, q$ and $1 \leq a \leq pq - 1$ such that $a$ is rel prime to $pq$, and $n$, return $a^n \pmod{pq}$.

Any op with numbers less than $pq$ takes 1 step; any op with a number BIGGER than $pq$, of length $L$, takes $L$ steps. Give an upper bound on the number of ops in terms of $n, p, q$. Can use $O$-notation.

**ANSWER**

1. Input$(a, n, p, q)$
2. Divide $n$ by $(p-1)(q-1)$ and take the remainder $r$. (This takes length $n$ which is $\lg(n)$ steps.)
3. We compute $a^r \pmod{pq}$ with repeated squaring. Since $r \leq pq$ this takes $\leq 2\lg(pq)$ steps.

This takes $\lg(n) + 2\lg(pq)$ steps.

# HW 06, Problem 5

Zelda does RSA with Alice1 and Alice2. With Alice1 she uses $N_1 = 91$ and $e = 2$. With Alice2 she uses $N_2 = 187$ and $e = 2$. Hence this is just the right setting for a low-$e$ attack.

Eve sees Zelda send Alice1 43.
Eve sees Zelda send Alice2 185.
Eve knows Zelda send SAME $m$ to Alice1 and Alice2.

Use the low-$e$ attack to find the message. Show all of your steps.

# HW 06, Problem 5, Solution

Let $m$ be the message. We know $m \leq 90$. We know
$m^2 \equiv 43 \pmod{91}$
$m^2 \equiv 185 \pmod{187}$
So we first seek an $x$ such that
$x \equiv 43 \pmod{91}$
$x \equiv 185 \pmod{187}$
$0 \leq x < 91 \times 187$.

$$x = 43 \times 187 \times (187^{-1} \pmod{91}) + 185 \times 91 \times (91^{-1} \pmod{187}).$$

$187 \pmod{91} = 5$. Need inverse of 5 mod 91. It's 93.
We need inverse of 91 mod 187. It's 37.

$$x = 43 \times 187 \times 73 + 185 \times 91 \times 37 = 1209888$$

We now mod this down by $187 \times 91 = 17017$ to get 1681.

$$m^2 \equiv 1681 \pmod{17017}.$$

Take $\sqrt{1681}$, its 41, so $m = 41$.