CSCI 2200
FOUNDATIONS OF COMPUTER SCIENCE

David Goldschmidt
goldsd3@rpi.edu
Fall 2022

We will review homework and problem set solutions in lecture on November 8 and in Problem Set 6 due on November 9

EXAM 2 LOGISTICS...

Exam 2 is on November 9 in our 6:00-7:50PM testblock in West Hall Auditorium
- If you have extra-time accommodations, I will email you further details regarding when/where
- **Please bring your RPI ID**

You can also bring one double-sided or two single-sided 8½"×11" cribsheets
- Feel free to collaborate on creating your cribsheets

Exam 2 will be graded out of 50 points
- We will have 18 multiple choice questions and three short answer questions
- Each multiple choice question will be worth 2 points—no partial credit—for a total of 36 points
- The three short answer questions will be worth 4 points, 5 points, and 5 points

Exam 2 covers everything through our November 4 lecture, i.e., through Chapter 11

To study for the exam, review both required and practice/warm-up problems (and solutions)...

Can Charlie decrypt M_1 from M_{1*} and avoid being eaten?

CRYPTOGRAPHY USING PRIMES

Alice and Bob are planning to kill Charlie because he is a tasty tuna…

Alice plans to send the coordinates M_1 of Charlie's location to Bob

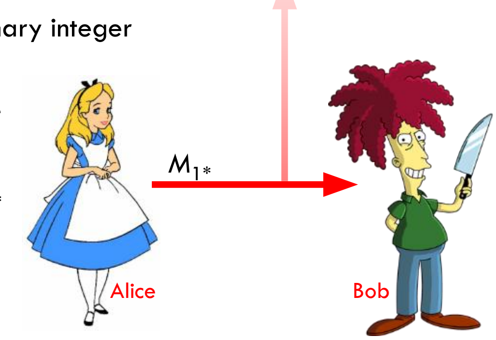
Alice got an A in FoCS, so she first encodes M_1 as a binary integer that is also a prime number (or as prime factors of M_1)

Alice also shared private key k with Bob ahead of time (k is a very large prime number)

Alice encrypts M_1 by setting $M_{1*} = M_1 \times k$, sending M_{1*}

Charlie is in RPISEC and intercepts the message

Bob did not take FoCS, but knows that $M_1 = M_{1*}/k$ (because Alice told him the formula to use)



CRYPTOGRAPHY USING PRIMES

Can Charlie decrypt M_1 from M_{1*} and avoid being eaten?

Charlie does not have k — but Charlie can determine the prime factorization of M_{1*} and obtain prime factors M_1 and k

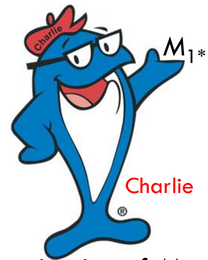
Charlie knows the message must be M_1 or k, so if he was quick enough, he survives…

Communication is secure only because prime factorization is inefficient

Knowing Charlie is on the move, Alice sends a second message $M_{2*} = M_2 \times k$

Charlie has M_{1*} and M_{2*} — how can he avoid being eaten?

CRYPTOGRAPHY USING PRIMES



Can Charlie decrypt M_1 from M_{1*} and avoid being eaten?

Charlie does not have k — but Charlie can determine the prime factorization of M_{1*} and obtain prime factors M_1 and k

Charlie knows the message must be M_1 or k, so if he was quick enough, he survives…

Communication is secure only because prime factorization is inefficient

Knowing Charlie is on the move, Alice sends a second message $M_{2*} = M_2 \times k$

Charlie has M_{1*} and M_{2*} — how can he avoid being eaten?

Charlie can quickly calculate gcd(M_{1*}, M_{2*}), which will simply be private key k (phew!)

```
e.g., k = 43 and M1 = 47

     M    = M   k   =  2021
      1*     1

     Charlie can do prime factorization
      and know that M1 is either 43 or 47

e.g., k = 43 and M2 = 73

     M    = M   k   =  3139
      2*     2

  gcd(2021, 3139) = gcd( 3139-2021, 2021)
                  = gcd( 1118, 2021 )
                  = gcd(  903, 1118 )
                  = ... = 43
```

MODULAR ARITHMETIC

What is the rightmost digit of 3^{2022}…?

n	1	2	3	4	5	6	7	8	9	10	…
3^n	3	9	27	81	243	729	2187	6561	19683	59049	…
last digit	3	9	7	1	3	9	7	1	3	9	7

The rightmost digit seems to repeat the sequence [3, 9, 7, 1] with a period of 4…

Since 2020 is a multiple of 4, the last digit of 3^{2022} is 9 (i.e., two "steps" beyond 3^{2020})

We define integers a and b to be *congruent modulo* integer d as follows:

$$a \equiv b \pmod{d} \quad \leftrightarrow \quad d \mid (a - b), \text{ i.e., } (a - b) = k \times d \text{ for some integer } k$$

e.g., $41 \equiv 79 \pmod{19}$ since $41 - 79 = k \times 19$ with $k = -2$

Does $111 \equiv 555 \pmod{12}$?

```
Does 111 equiv 555 (mod 12)?

Yes, 111 - 555 = -444 = 12k

                         k = -37


Is 111 equiv 555 (mod 12) the same as
   555 equiv 111 (mod 12) ...?

Yes, 555 - 111 = 444 = 12k

                      k = 37
```

MODULAR ARITHMETIC

We define integers a and b to be *congruent modulo* integer d as follows:

$a \equiv b \pmod{d} \quad \leftrightarrow \quad d \mid (a - b)$, i.e., $(a - b) = k \times d$ for some integer k

In other words, a and b have the same remainder when divided by d…

This *congruence relation* is an *equivalence relation* since it meets these three requirements:

Reflexive — $a \equiv a \pmod{d}$ *Symmetric* — $a \equiv b \pmod{d} \leftrightarrow b \equiv a \pmod{d}$

Transitive — if $a \equiv b \pmod{d}$ and $b \equiv c \pmod{d}$, then $a \equiv c \pmod{d}$

What about addition, subtraction, multiplication, exponentiation, etc.?

For addition, if $a \equiv b \pmod{d}$ and $r \equiv s \pmod{d}$, does $a + r \equiv b + s \pmod{d}$…?

```
 We know 111 equiv 555 (mod 12)
+ and     25 equiv  37 (mod 12)
-------------------------------
         136 equiv 592 (mod 12) ???
  rem(136,12) = 4 and rem(592,12) = 4
    12|(136-592) ???
```

MODULAR ARITHMETIC

We define integers *a* and *b* to be *congruent modulo* integer *d* as follows:

$$a \equiv b \pmod{d} \quad \leftrightarrow \quad d \mid (a - b), \text{ i.e., } (a - b) = k \times d \text{ for some integer } k$$

This *congruence relation* is an *equivalence relation* since it meets these three requirements:

Reflexive — $a \equiv a \pmod{d}$ *Symmetric* — $a \equiv b \pmod{d} \leftrightarrow b \equiv a \pmod{d}$

Transitive — if $a \equiv b \pmod{d}$ and $b \equiv c \pmod{d}$, then $a \equiv c \pmod{d}$

Prove each of these via a direct proof…

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$. Then,

(a) $ar \equiv bs \pmod{d}$. (b) $a + r \equiv b + s \pmod{d}$. (c) $a^n \equiv b^n \pmod{d}$.

```
Given a equiv b (mod d) and
      r equiv s (mod d), which means
      a = b + kd  and  r = s + ld

Prove ar equiv bs (mod d)...

   d|(ar - bs)  ???
   d|((b + kd)(s + ld) - bs)
   d|((bs + bld + skd + kld^2) - bs)
   d|(bld + skd + kld^2)
   d|d(bl + sk + kld)
```

MODULAR ARITHMETIC

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$. Then,

(a) $ar \equiv bs \pmod{d}$. (b) $a + r \equiv b + s \pmod{d}$. (c) $a^n \equiv b^n \pmod{d}$.

What is the rightmost digit of 3^{2022}...?

For 3^n, the rightmost digit repeats the sequence [3, 9, 7, 1] with a period of 4

$$\begin{aligned} 3^2 &\equiv -1 \pmod{10} \\ 3^{2k} &\equiv (-1)^k \pmod{10} && \text{[exponent } n = 2k \text{ is even]} \\ 3^{2k+1} &\equiv (-1)^k \times 3 \pmod{10} && \text{[exponent } n = 2k+1 \text{ is odd]} \end{aligned}$$

What pattern emerges here for the rightmost digit...?

MODULAR ARITHMETIC

For 3^{2022}, $k = 1011$, so n is even and $\lfloor n/2 \rfloor$ is odd...
...and therefore $3^{2022} \equiv -1 \pmod{10} \equiv 9$

What is the rightmost digit of 3^{2022}...?

For 3^n, the rightmost digit repeats the sequence [3, 9, 7, 1] with a period of 4

$$\begin{aligned} 3^2 &\equiv -1 \pmod{10} \\ 3^{2k} &\equiv (-1)^k \pmod{10} && \text{[exponent } n = 2k \text{ is even]} \\ 3^{2k+1} &\equiv (-1)^k \times 3 \pmod{10} && \text{[exponent } n = 2k+1 \text{ is odd]} \end{aligned}$$

$$3^n \equiv \begin{cases} 1 \pmod{10} & \text{if } n \text{ is even and } \lfloor n/2 \rfloor \text{ is even} \\ -1 \pmod{10} & \text{if } n \text{ is even and } \lfloor n/2 \rfloor \text{ is odd} \\ 3 \pmod{10} & \text{if } n \text{ is odd and } \lfloor n/2 \rfloor \text{ is even} \\ -3 \pmod{10} & \text{if } n \text{ is odd and } \lfloor n/2 \rfloor \text{ is odd} \end{cases}$$

```
 2021     2020+1
3      = 3

     k = 1010

  n = 2k + 1 is odd
  and floor( n/2 ) is even

 2021
3      = 3 (mod 10) = 3
                      ^^^
               the rightmost digit
```

MODULAR ARITHMETIC

What is the remainder when 5^{2015} is divided by 3? …divided by 7? …divided by 9?

Tinker to determine that $5^2 \equiv 1 \pmod 3$, then raise both sides to the n power…

$$5^{2n} \equiv 1^n \pmod 3$$

$$5^{2(1007)} \equiv 1^{1007} \pmod 3 \qquad \text{[exponent } 2n = 2014\text{]}$$

$$5^{2(1007)+1} \equiv 1 \times 5 \pmod 3 \equiv 2 \qquad \text{[remainder is 2]}$$

$18 \times 7 - 1 = 5^3$

For 5^{2015} divided by 7, tinker to find that $5^3 \equiv -1 \pmod 7$…

$$5^{3n} \equiv (-1)^n \pmod 7$$

$$5^{3(671)} \equiv (-1)^{671} \pmod 7 \qquad \text{[exponent } 3n = 2013\text{]}$$

$$5^{3(671)+2} \equiv -25 \pmod 7 \equiv 3 \qquad \text{[remainder is 3]}$$

we are 3 away from −28

MODULAR DIVISION

Modular division is very different than regular division…

$$15 \times 6 \equiv 13 \times 6 \pmod{12}$$
$$15 \not\equiv 13 \pmod{12}$$ ✘

$$15 \times 6 \equiv 2 \times 6 \pmod{13}$$
$$15 \equiv 2 \pmod{13}$$ ✓

A prime modulus always works…

$$7 \times 8 \equiv 52 \times 8 \pmod{15}$$
$$7 \equiv 52 \pmod{15}$$ ✓

A composite modulus only works sometimes…

Modular Division: cancelling a factor from both sides

Suppose $ac \equiv bc \pmod{d}$. You can cancel c to get $a \equiv b \pmod{d}$ if $\gcd(c, d) = 1$.

Can you prove this…?

MODULAR DIVISION

Modular division is very different than regular division…

$$15 \times 6 \equiv 13 \times 6 \pmod{12}$$
$$15 \not\equiv 13 \pmod{12}$$ ✘

$$15 \times 6 \equiv 2 \times 6 \pmod{13}$$
$$15 \equiv 2 \pmod{13}$$ ✓

$$7 \times 8 \equiv 52 \times 8 \pmod{15}$$
$$7 \equiv 52 \pmod{15}$$ ✓

Modular Division: cancelling a factor from both sides

Suppose $ac \equiv bc \pmod{d}$. You can cancel c to get $a \equiv b \pmod{d}$ if $\gcd(c, d) = 1$.

Proof. $d \mid c(a-b)$. By GCD fact (v), $d \mid a-b$ because $\gcd(c, d) = 1$. ■

(v) IF $d \mid mn$ AND $\gcd(d, m) = 1$, THEN $d \mid n$.

MODULAR MULTIPLICATIVE INVERSE

For our cryptography problem, we need a multiplicative inverse for decryption...

We define a modulus d such that for integer k, the *modular multiplicative inverse* k^{-1} satisfies both
$$\begin{cases} 1 \leq k^{-1} < d \\ k^{-1} \times k \equiv 1 \pmod{d} \end{cases}$$

e.g., for modulus $d = 6$, what is multiplicative inverse 35^{-1}?

For modulus $d = 6$, multiplicative inverse $35^{-1} = 5$ because $5 \times 35 = 175 \equiv 1 \pmod{6}$

e.g., for modulus $d = 6$, what is multiplicative inverse 15^{-1}?

MODULAR MULTIPLICATIVE INVERSE

For our cryptography problem, we need a multiplicative inverse for decryption...

We define a modulus d such that for integer k, the *modular multiplicative inverse* k^{-1} satisfies both
$$\begin{cases} 1 \leq k^{-1} < d \\ k^{-1} \times k \equiv 1 \pmod{d} \end{cases}$$

e.g., for modulus $d = 6$, what is multiplicative inverse 15^{-1}?

For $d = 6$, multiplicative inverse 15^{-1} does not exist since if it did, then $15k \equiv 1 \pmod{6}$...

...or $15k - 6a = 1$ — rewriting this as $3(5k - 2a) = 1$, we see that this is impossible!

The modular multiplicative inverse may not exist for all $k \neq 0$...

MODULAR MULTIPLICATIVE INVERSE

Prove this using Bezout's Identity…

Theorem 10.10. The inverse of k exists modulo d iff $\gcd(k, d) = 1$.

When $\gcd(k, d) = 1$, use Bezout's Identity to obtain $kx + dy = 1$ — from this, $k^{-1} = \text{rem}(x, d)$

e.g., compute 12^{-1} for modulus $p = 17$…

$$\begin{aligned} \gcd(12, 17) &= \gcd(5, 12) && \Rightarrow 5 = -12 + 17 \\ &= \gcd(2, 5) && \Rightarrow 2 = 12 - 5 \times 2 = 12 - (17 - 12) \times 2 = 3 \times 12 - 2 \times 17 \\ &= \gcd(1, 2) && \Rightarrow 1 = 5 - 2 \times 2 = -7 \times 12 - 5 \times 17 \end{aligned}$$

Therefore, $12^{-1} = \text{rem}(-7, 17) = 10$ — double-check that $12 \times 10 = 120 \equiv 1 \pmod{17}$

e.g., compute 8^{-1} for modulus $p = 19$…

MODULAR MULTIPLICATIVE INVERSE

Prove this using Bezout's Identity…

Theorem 10.10. The inverse of k exists modulo d iff $\gcd(k, d) = 1$.

When $\gcd(k, d) = 1$, use Bezout's Identity to obtain $kx + dy = 1$ — from this, $k^{-1} = \text{rem}(x, d)$

e.g., compute 8^{-1} for modulus $p = 19$…

$$\begin{aligned} \gcd(8, 19) &= \gcd(3, 8) && \Rightarrow 3 = -8 \times 2 + 19 \\ &= \gcd(2, 3) && \Rightarrow 2 = 8 - 3 \times 2 = 8 - (-8 \times 2 + 19) \times 2 = 8 \times 5 - 2 \times 19 \\ &= \gcd(1, 2) && \Rightarrow 1 = 3 - 2 = -7 \times 8 + 3 \times 19 \end{aligned}$$

Therefore, $8^{-1} = \text{rem}(-7, 19) = 12$ — double-check that $12 \times 8 = 96 \equiv 1 \pmod{19}$

Check out Fermat's Little Theorem (Exercise 10.14) for an even quicker method…

Can Charlie decrypt M from M_* and avoid being eaten?

RSA PUBLIC KEY CRYPTOGRAPHY

Rivest, Shamir, and Adleman (RSA), 1977

Alice and Bob are planning to kill Charlie because he is a tasty tuna…

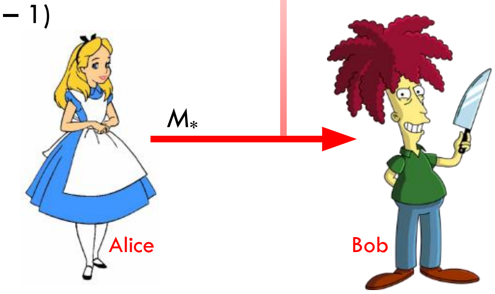
Bob defines $n = p \times q$, where p and q are two large prime numbers

Bob defines e such that $\gcd(e, (p-1)(q-1)) = 1$ and computes private key d as the modular inverse of e for modulus $(p-1)(q-1)$

With both n and e as public keys, Alice computes $M_* \equiv M^e \pmod{n}$, then sends M_* to Bob

Charlie intercepts the message…

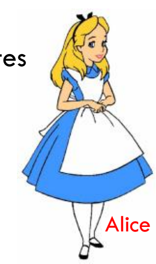
Bob uses private key d to decrypt M_* by computing $M \equiv M_*^d \pmod{n}$



RSA PUBLIC KEY CRYPTOGRAPHY

e.g., message $M = 241$, modulus $n = 391$, and power $e = 225$ — then, Alice computes

$$M_* \equiv M^e \pmod{n} \equiv 241^{225} \pmod{391}$$



Repeatedly halve the power…

$$\left.\begin{aligned} 241^{225} &\equiv 241 \times (241^{112})^2 \\ 241^{112} &\equiv (241^{56})^2 \\ 241^{56} &\equiv (241^{28})^2 \\ 241^{28} &\equiv (241^{14})^2 \\ 241^{14} &\equiv (241^{7})^2 \\ 241^{7} &\equiv 241 \times (241^{3})^2 \\ 241^{3} &\equiv 112 \end{aligned}\right\} \pmod{391}$$

…then substitute back in

$$\left.\begin{aligned} 241^{3} &\equiv 112 \\ 241^{7} &\equiv 241 \times 112^2 \equiv 283 \\ 241^{14} &\equiv 283^2 \equiv 325 \\ 241^{28} &\equiv 325^2 \equiv 55 \\ 241^{56} &\equiv 55^2 \equiv 288 \\ 241^{112} &\equiv 288^2 \equiv 52 \\ 241^{225} &\equiv 241 \times 52^2 \equiv 258 \end{aligned}\right\} \pmod{391}$$

M_*

RSA PUBLIC KEY CRYPTOGRAPHY

How does Bob decrypt M_* to obtain message M?

e.g., $M_* = 258$, modulus $n = 391$, and private key $d = 97$ — then, Bob computes

$$M \equiv M_*^d \pmod{n} \equiv 258^{97} \pmod{391}$$

Bob

Do this exercise to make sure Bob successfully obtains original message M

Charlie

Can Charlie decrypt M from M_* and avoid being eaten?

GRAPHY

ge M?

ate key $d = 97$ — then, Bob computes

$\equiv 258^{97} \pmod{391}$

Bob

e sure Bob successfully obtains original message M

and avoid being eaten?

https://www.youtube.com/watch?v=Y4LLj6EQZCY

WHAT NEXT…?

Homework 4 has been posted and is due by 11:59PM on Thursday, November 3

Recitations tomorrow (November 2) are optional Q&A sessions focused on Homework 4

Problem Set 6 will be posted at the end of this week…

- …and due in your recitations **next week** on Wednesday, November 9

Earning late days has still not been tallied, so still assume you have earned them even though you do not yet see them in Submitty…

Practice! Tinker! Practice! Tinker! Practice! Tinker! Practice! Tinker! Practice!