LOVE LETTERS,
M & M’s,
and
CIRCE’S CAVE
NUMBER THEORY
SOME USES OF NUMBER THEORY IN COMMUNICATION AND NETWORK SECURITY

- You can verify someone’s identity
- You can verify that a message has not been altered
- You can verify that a message comes from the one who signs it
- You can have a secret conversation with someone, even if you don’t trust each other
- Anyone can send you a secret message that nobody but you can read
- You can prove that you know a secret without having to tell it
Some Number Theory We’ll Need:

- **Divisor:** a number which leaves no remainder when you divide it into a given number (6 is a divisor of 24 but not of 15)

- **Prime:** a number bigger than 1 with no positive divisors except itself and 1 — for example, 3, 17 and 2147483647

- $a \pmod{n}$: the remainder when you divide $a$ by $n$

- $a \equiv b \pmod{n}$: $n$ is a divisor of $a - b$
Facts About Powers And Roots \( (\mod n) \)

- It’s pretty easy to calculate \( s^2 \mod n \), if you know \( s \) and \( n \). For example:

\[
\begin{align*}
  s &= 7499333456034068, \quad n = 147573952589676412927 \\
  s^2 &= 56240002284791878520359176628624 \\
  &= 381097079111 \cdot n + 1003261227554560727,
\end{align*}
\]

so \( 7499333456034068^2 \equiv 1003261227554560727 \mod n \).

But if \( n \) is a product of two primes, it’s hard to calculate \( s \) if I just tell you the value of \( s^2 \) \( (\mod n) \) and \( n \) is really big. For example, if

\[
\begin{align*}
  n &= 147573952589676412927, \quad \text{and} \\
  s^2 &= 99611274043958415426 \mod n,
\end{align*}
\]

it is a hard problem to find \( s \) — unless I also tell you the two prime factors of \( n \). And I’m not telling.

Oh, I’ll tell. They are 193707721 and 761838257287.

Similarly, if I tell you that

\[
5^k \equiv 211315043454597681946123 \mod 467972643709352841894517,
\]

to find the value of \( k \) is very hard.

Oh, all right; \( k = 17387387947 \). But don’t tell.
The M&M’s Key Exchange On A Computer: The Diffie–Hellman Key Exchange

Common Information:

- A large prime number $p$
- A number $s < p$ with no factors in common with $p - 1$

NATASHA  
Chooses $n < p$ (secret)  
Computes $N \equiv s^n \pmod{p}$  
Sends $N$ to Boris  
Computes $B^n \pmod{p}$

BORIS  
Chooses $b < p$ (secret)  
Computes $B \equiv s^b \pmod{p}$  
Sends $B$ to Natasha  
Computes $N^b \pmod{p}$

Because

$$B^n \equiv (s^b)^n \equiv s^{bn} \equiv s^{nb} \equiv (s^n)^b \equiv N^b \pmod{p},$$

Boris and Natasha now have a common key.
Advantages of Diffie–Hellman

- The prime \( p \) and the number \( s \) are made public, so anyone can use them.

- The only secret number is the user’s exponent (Natasha’s number \( n \) and Boris’ number \( b \)).

- It only uses arithmetic, and so it can easily be used on all kinds of machines.

- Natasha and Boris can still communicate, even though they will not trust each other with a key.

- Knowing both \( s \) and \( s^n \pmod{p} \) gives you no useful information about \( n \) — nobody knows a fast (or even moderately fast) way to break this system.
VERIFYING A PERSON’S IDENTITY

People Can Be Identified By Their —

- **Attributes:** Looks, Voice, Walk, Mannerisms, Habits, Fingerprints, Voice Prints, Blood Types, Brain Scans, DNA
  - By Other People: Easy and common
  - By Computer: Difficult

- **Possessions:** Identification Papers, Driver’s License, Credit Card, Birth Certificate, ID Badge, Letter of Reference, Passport
  - By Other People: Common
  - By Computer: Possible

- **Knowledge:** Passwords, Special Questions, Pass Phrases
  - By Other People: Uncommon
  - By Computer: Simple
Convincing Someone That You Know A Secret Without Telling:

CIRCE’S CAVE

Entrance

North Door

Secret Door

Hall

South Door

- Ulysses decides by a coin flip whether Circe should use the North Door or the South Door
- If Circe knows the secret, she uses the right door every time
- If Circe doesn’t know the secret, she has only one chance in 1,048,576 of using the right door 20 times in a row
HOW A COMPUTER VERIFIES A PERSON’S IDENTITY

- You are verified if you have the right key — a password or secret number.
- Computer challenges you to compute something using your key.
- It does the same with what it thinks is your key.
- If they match, you’re in!
- Key is never sent, only some computation using it.
- Computation depends on random numbers the computer gives you.

A PROBLEM —

You might have to do complex calculations yourself.

SOLUTION — THE SMART CARD!
TWO–STAGE IDENTIFICATION WITH A SMART CARD

- You identify yourself to the Smart Card — usually a secret number (such as the PIN number for an ATM card)

- The Smart Card identifies itself to the computer — using some sort of interactive routine. Our routine uses arithmetic.

- We can use those facts about powers and roots — in particular, squares and square–roots — to invent an identification routine for a Smart Card that is interactive and uses number theory.
A Smart Card Routine Using Number Theory

Computer knows:

- Two large primes $p$ and $q$ (kept secret)
- A secret number $s$ for the Smart Card

Smart Card knows:

- $n = pq$
- The secret number $s$
- $v \equiv s^2 \pmod{n}$ — the Card uses this number and never has to tell what $s$ is

The Routine
(can be done many times)

- Card picks a number $r$ at random, calculates $x \equiv r^2 \pmod{n}$ and sends $x$ to Computer.
- Computer flips a coin.
- If the coin flip is Heads, Card sends $r$ to Computer.
- Computer calculates $r^2 \pmod{n}$. If it gets $x$, Card is accepted. If not, Card is rejected.
- If the coin flip is Tails, Card sends $rs$ to Computer.
- Computer calculates $(rs)^2 \pmod{n}$. If it gets $xv$, Card is accepted. If not, Card is rejected.