Discrete Structures

Day 6

Proof of RSA

Cipher text $C = M^e mod\ n$

Plain text M $= C^d mod\ n$

Assume that the plaintext retrieved by Bob is M_1. We need to prove that $M_1 = M$.

$$M_1 = C^d mod\ n = (M^e\ mod\ n)^{\ d} mod\ n$$

$$M_1 = M^{ed}\ mod\ n$$

We know $d \equiv e^{-1} \mathrm{mod} \varphi(n)$ or $d \times e \equiv 1 \bmod \varphi(n)$.

$d \times e = k \times \varphi(n) + 1$, where k is an integer.

$$M_1 = M^{k \times \varphi(n) + 1}\ mod\ n$$

Second version of Euler's theorem: If $n = p \times q, a < n$ and k is an integer, then $a^{k \times \varphi(n) + 1} \equiv a\ mod\ n$.

$$M_1 = M\ mod\ n$$

512 bit prime:

p=6703903964971298549787012499102923063739682910296196688861780721860882015036773488400937149083451713845015929093243025426876941405973284973216824503042159;

q=6703903964971298549787012499102923063739682910296196688861780721860882015036773488400937149083451713845015929093243025426876941405973284973216824503042857;

n=449423283715578976932326297697256183404494244735576643183575202894331689513752407831771193306018840052800284699678483394146974422036041556232118576598746986860897469508821753705747295895301640381407432389750042804736496820394495519778071398123635848675750423259123581433795382707134244983841985609485480826 3.

Possible number of ‘e’ = 6.34423×10^{304} (approx.)

Number of people: 8,000,000,000 (approx.).

Propositional Logic

- Logic is the basis of all mathematical reasoning and of all automated reasoning.
- **Propositions:** A **proposition** is a declarative sentence (that is, a sentence that declares a fact) that is either true or false, but not both. A proposition ia a basic building blocks of logic.

  - Eg:
    - 1 + 1 = 2.
    - Toronto is the capital of Canada.
    - What time is it?
    - $x + 1 = 2$.

- **Propositional variables** (or **statement variables**): Variables that represent propositions. The conventional letters used for propositional variables are *p, q, r, s, ...*
- If the proposition is true, it is denoted by T. If the proposition is false, it is denoted by F.
- The area of logic that deals with propositions is called the **propositional calculus** or **propositional logic**.

- Many mathematical statements are constructed by combining one or more propositions. New propositions, called **compound propositions**, are formed from existing propositions using logical operators.

1. ***Negation of p***: Let p be a proposition. The *negation of p*, denoted by $\neg p$ (also denoted by $\overline{p}$) read as "not p", is the statement "It is not the case that p."

- Eg: Find the negation of the proposition

  "Michael's PC runs Linux"

  and express this in simple English.

"It is not the case that Michael's PC runs Linux."

"Michael's PC does not run Linux."

Truth table

p	$\neg p$
T	F
F	T

Q. Find the negation of the proposition

"Vandana's smartphone has at least 32GB of memory"

and express this in simple English.

"It is not the case that Vandana's smartphone has at least 32GB of memory."

"Vandana's smartphone does not have at least 32GB of memory"

"Vandana's smartphone has less than 32GB of memory."

2. *Conjunction* of *p* and *q:* Let *p* and *q* be propositions. The *conjunction* of *p* and *q*, denoted by $p \wedge q$, is the proposition "*p* and *q*." The conjunction $p \wedge q$ is true when both *p* and *q* are true and is false otherwise.

Truth table

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

3. *Disjunction* of *p* and *q:* Let *p* and *q* be propositions. The *disjunction* of *p* and *q*, denoted by $p \vee q$, is the proposition "*p* or *q*." The disjunction $p \vee q$ is false when both *p* and *q* are false and is true otherwise.

Truth table

p	q	$p \vee q$	$p \oplus q$
T	T	T	F
T	F	T	T
F	T	T	T
F	F	F	F

4. *Exclusive or* of *p* and *q:* Let *p* and *q* be propositions. The *exclusive or* of *p* and *q*, denoted by $p \oplus q$, is the proposition that is true when exactly one of *p* and *q* is true and is false otherwise.

5. Conditional Statements: Let p and q be propositions. The *conditional statement* $p \rightarrow q$ is the proposition "if p, then q." The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise.

In the conditional statement $p \rightarrow q$, p is called the *hypothesis* (or *antecedent* or *premise*) and q is called the *conclusion* (or *consequence*). A conditional statement is also called an **implication**.

- Note that the statement $p \rightarrow q$ is true when both p and q are true and when p is false (no matter what truth value q has).
- "If you get 100% on the final, then you will get an A."

Truth table

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Truth table

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Expressing conditional statement:

1. “if p, then q”
2. “p implies q”
3. “if p, q”
4. “p only if q”
5. “p is sufficient for q”
6. “a sufficient condition for q is p”
7. “q if p”
8. “q whenever p”
9. “q when p”
10. “q is necessary for p”
11. “a necessary condition for p is q”
12. “q follows from p”
13. “q unless $\neg p$”

Q. Let p be the statement "Maria learns discrete mathematics" and q the statement "Maria will find a good job." Express the statement $p \rightarrow q$ as a statement in English.

p: Maria learns discrete mathematics.

q: Maria will find a good job.

"if p, then q"

"If Maria learns discrete mathematics, then she will find a good job."

"q when p"

"Maria will find a good job when she learns discrete mathematics."

"q unless $\neg p$"

"Maria will find a good job unless she does not learn discrete mathematics."

CONVERSE, CONTRAPOSITIVE, AND INVERSE

CONVERSE: **The converse** of $\mathrm{p} \rightarrow q$ is the proposition $\mathrm{q} \rightarrow p$.

CONTRAPOSITIVE: The **contrapositive** of $\mathrm{p} \rightarrow q$ is the proposition $\neg q \rightarrow \neg p$.

INVERSE: The **inverse** of $\mathrm{p} \rightarrow q$ is the proposition $\neg \mathrm{p} \rightarrow \neg q$.

Q. Find the truth table for converse, contrapositive and inverse:

p	q	Converse: $\mathrm{q} \rightarrow p$	Contrapositive: $\neg q \rightarrow \neg p$	Inverse: $\neg \mathrm{p} \rightarrow \neg q$
T	T			
T	F			
F	T			
F	F			

Only the contrapositive always has the same truth value as $p \rightarrow q$. When two compound propositions always have the same truth value we call them **equivalent**. A conditional statement and its contrapositive are equivalent.

Q. What are the contrapositive, the converse, and the inverse of the conditional statement

“The home team wins whenever it is raining?”

“*q* whenever *p*”

q: The home team wins

p: It is raining.

“The home team wins whenever it is raining?”

“*q* whenever *p*”

q: The home team wins

p: It is raining.

Contrapositive $\neg q \rightarrow \neg p$: “If the home team does not win, then it is not raining.”

Converse $\mathrm{q} \rightarrow p$: “If the home team wins, then it is raining.”

Inverse $\neg \mathrm{p} \rightarrow \neg q$: “If it is not raining, then the home team does not win.”

BICONDITIONALS: Let p and q be propositions. The *biconditional statement*

$p \leftrightarrow q$ is the proposition "p if and only if q." Biconditional statements are also called *bi-implications*.

$p \leftrightarrow q$ has exactly the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$.

Q. Find the truth table for $p \leftrightarrow q$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
T	T			
T	F			
F	T			
F	F			

Q. Let p be the statement "You can take the flight," and let q be the statement "You buy a ticket."

Then $p \leftrightarrow q$ is the statement?

Q. Construct the truth table of the compound proposition

$(p \vee \neg q) \rightarrow (p \wedge q)$.

Precedence of Logical Operators

Operator	Precedence
¬	1
∧	2
∨	3
→	4
↔	5

Q. Let p, q, and r be the propositions

p :You have the flu.

q :You miss the final examination.

r :You pass the course.

Express each of these propositions as an English sentence.

a) $p \rightarrow q$ **b)** $\neg q \leftrightarrow r$

c) $q \rightarrow \neg r$ **d)** $p \vee q \vee r$

e) $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$

f) $(p \wedge q) \vee (\neg q \wedge r)$

Sometimes in logic, the word “but” is used instead of “and”.

The sun is shining, but it is raining.

Expressing it using logical connective:

p: The sun is shining.

q: It’s raining

$$p \wedge q$$

Q. Let p, q, and r be the propositions

p : Grizzly bears have been seen in the area.

q : Hiking is safe on the trail.

r : Berries are ripe along the trail.

Write these propositions using p, q, and r and logical connectives (including negations).

a) Berries are ripe along the trail, but grizzly bears have not been seen in the area.

b) Grizzly bears have not been seen in the area and hiking on the trail is safe, but berries are ripe along the trail.

c) If berries are ripe along the trail, hiking is safe if and only if grizzly bears have not been seen in the area.

d) It is not safe to hike on the trail, but grizzly bears have not been seen in the area and the berries along the trail are ripe.

e) Hiking is not safe on the trail whenever grizzly bears have been seen in the area and berries are ripe along the trail.