Lecture #1 Midterm – Probability of Events, Cryptography, & Bayes' Theorem (March 8, 2023)

REMINDERS!

1) ALWAYS FOLLOW MY CLASSROOM PROCEDURES.
2) ACTIVITIES ARE ALWAYS UPDATED IN GOOGLE CLASSROOM, & MYOPENMATH
3) ALWAYS SUBMIT YOUR WORK ON TIME. NO MORE SUBMISSSION OF LATE WORK.
4) THE WEEKLY HOMEWORK IS ALWAYS DUE EVERY SATURDAY at 10:00 AM
5) CHECK THE UPDATES ON GOOGLE CLASSROOM AND DO YOUR MISSING ASSIGNMENTS as the GRADES are always UPDATED.

Note: **Activities that you failed to submit on-time will automatically disappear on the system.**

MyOpenMath

1) Bellwork 1 (Midterm) – All That You Know 03.08.23
2) Activity #1 (Midterm) – It is Probability All About Probability, Permutations, and Combinations 03.08.23 ***(Due Date: March 09, 2023, 11:59 PM)***
3) Weekly Homework # 1 (Midterm) – Recalling Knowledge is a MUST 03.08-14.23 ***(Due Date: March 14, 2023, 10:00 AM)***

Google Classroom

1) Lecture Notes for Today 13.08.23

At the end of the lesson, students will be able to:
1) solve probability problems

Basic Counting Principles

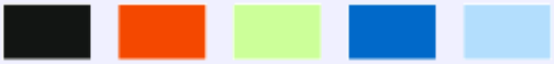
The Basic Counting Rule is used for scenarios that have multiple choices or actions to be determined.

The rule that states that when there are ***m*** ways to do one thing, and ***n*** ways to do another, then altogether there are ***m x n*** ways of doing both.

There are **2** body styles:

sedan or hatchback

There are **5** colors available:

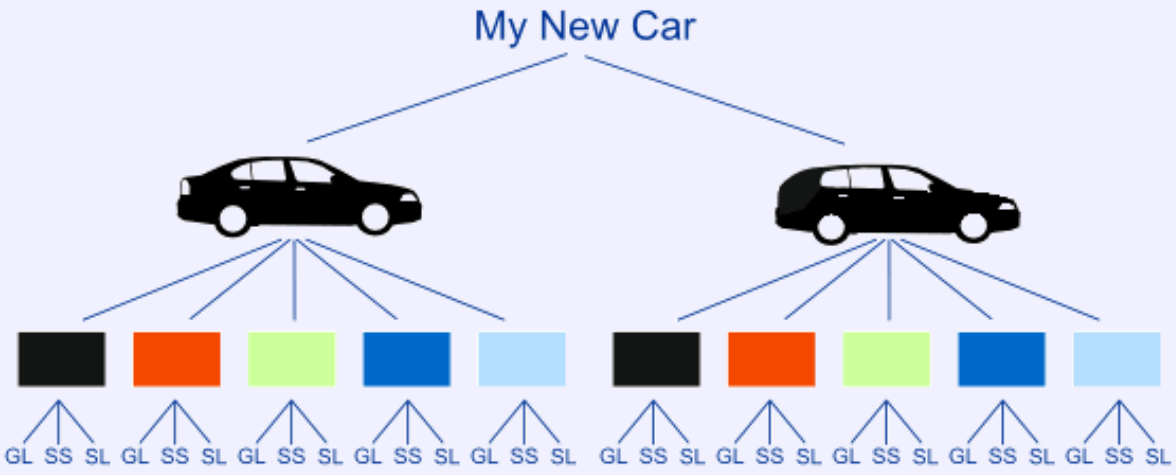


There are **3** models:

- GL (standard model),
- SS (sports model with bigger engine)
- SL (luxury model with leather seats)

How many total choices?

You can see in this "tree" diagram:



You can count the choices, or just do the simple calculation:

Total Choices = 2 × 5 × 3 = 30

1) Sum Rule Principle: Assume some event *E* can occur in m ways and a second event *F* can occur in n ways and suppose both events cannot occur simultaneously. Then E ***or*** F can occur in m + n ways.

In general, if there are n events and no two events occurs in same time then the event can occur in $n_1 + n_2 \ldots\ldots\ldots n_j$ ways.

Example: If 8 male professors and 5 female professors teaching Discrete Structures, then the student can choose professor in ***8+5=13 ways.***

2) Product Rule Principle: Suppose there is an event E which can occur in m ways and, independent of this event, there is a second event F which can occur in n ways. Then combinations of E and F can occur in m x n ways.

In general, if there are n events occurring independently then all events can occur in the order indicated as $n_1 \times n_2 \times n_3 \ldots\ldots\ldots n_j$ ways.

Example: In class, there are 4 boys and 10 girls if a boy and a girl have to be chosen for the class monitor, the students can choose class monitor in $4 \times 10 = 40$ ways.

EXTRA EXAMPLE 1: If a boy owns 2 pairs of pants, 3 shirts, 8 ties, and 2 jackets. How many different outfits can he wear if he must wear one of each item?

EXTRA EXAMPLE 2: If a girl owns 3 pairs of blouses, 6 shirts, 2 ties, 2 jackets, and 3 pairs of shoes. How many different outfits can she wear if she must wear one of each item?

I DO 1) A license plate is to have the following form: ***three letters followed by three numbers.*** An example of a license plate like this would be MTH 314. How many different license plates can be made, assuming that ***letters and numbers can be reused?***

YOU DO 1) License plates in the state of Maryland are in the following form: one number (which cannot be zero), two letters, four numbers (which includes zero). For instance, a valid plate is 4MD1234

WE DO 1) Standard automobile license plates in a country display 2 numbers, followed by 3 letters, followed by 2 numbers. How many different standard plates are possible in this system? (Assume repetitions of letters and numbers are allowed.)

Factorial

Definition

The factorial of a non–negative integer n, denoted by $n!$, is the product of all positive integers less than or equal to n.

Example:

$$5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$$

Convention:

$$0! = 1$$

EXTRA EXAMPLE 1)

How many three-letter "words" can be made from 7 letters "FGHIJKL" if repetition of letters

(a) is allowed?

There are [ ] possible three-letter "words".

(b) is not allowed?

There are [ ] possible three-letter "words".

Question Help: Video Video

EXTRA EXAMPLE 2)

A true-false test contains 19 questions. In how many different ways can this test be completed. (Assume we don't care about our scores.)

Your answer is :

Question Help: Video

EXTRA EXAMPLE 3)

A child rolls 3 standard dice of different colors and records the numbers showing. Find the number of different outcomes.

EXTRA EXAMPLE 4)

Find the number of different finishes for a race with 7 runners. (Assume no ties occur.)

EXTRA EXAMPLE 5)

In how many ways can first, second, and third prizes be awarded in a contest with 615 contestants?

Question Help: Video

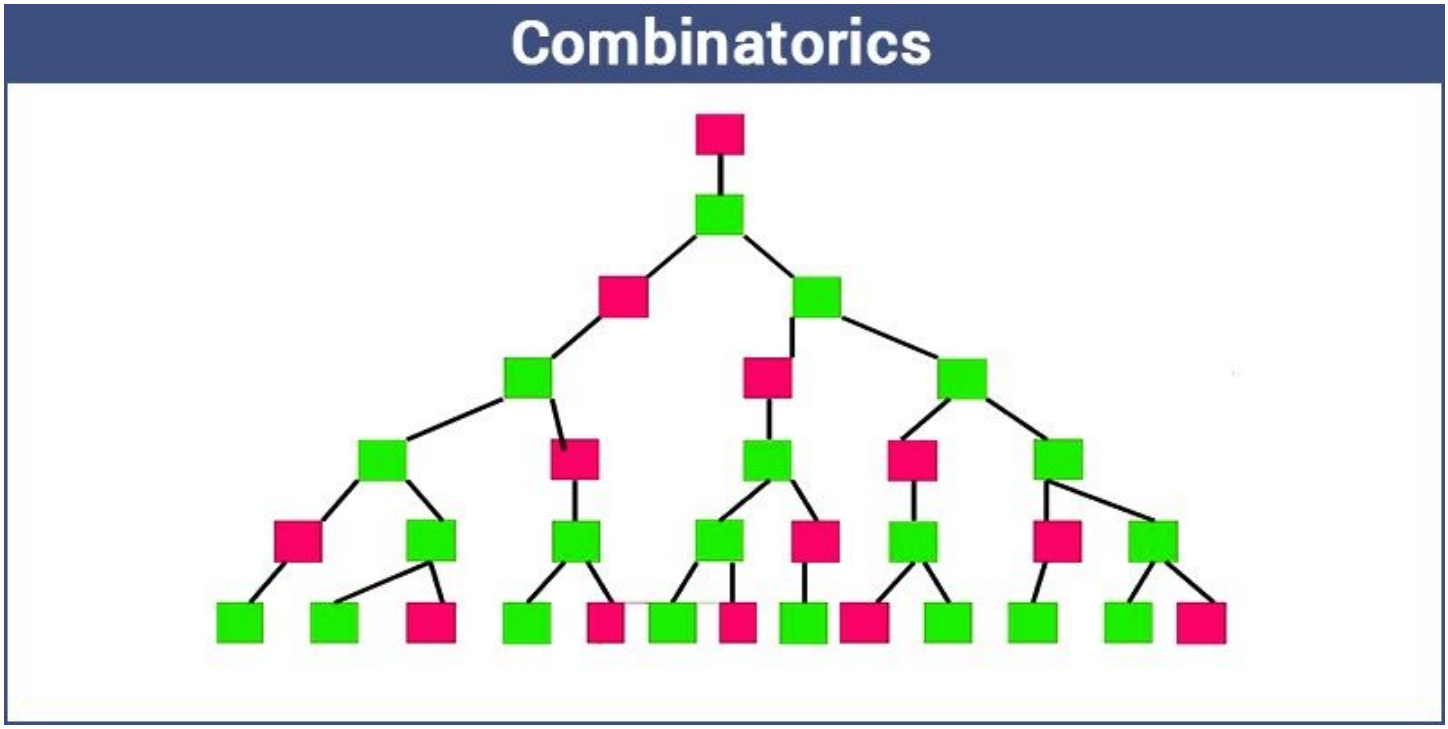
Source: ***https://byjus.com/maths/combinatorics/***

Combinatorics

Combinatorics is a stream of mathematics that concerns the study of finite discrete structures. It deals with the study of ***permutations and combinations,*** enumerations of the sets of elements. It characterizes Mathematical relations and their properties.

Mathematicians uses the term ***"Combinatorics"*** as it refers to the larger subset of Discrete Mathematics. It is frequently used in computer Science to derive the formulas and it is used for the estimation of the analysis of the algorithms. In this lesson, let us discuss what is combinatorics, its features, formulas, applications, and examples in details.

Features of combinatorics



Some of the important features of the combinatorics are as follows:

- Counting the structures of the provided kind and size.
- To decide when criteria can be fulfilled and analyzing elements of the criteria, such as combinatorial designs.
- To identify “greatest”, “smallest” or “optimal” elements, known as external combinatorics.

Key Idea. Combinatorial structures that rise in an algebraic concept, or applying algebraic techniques to combinatorial problems, known as algebraic combinatorics.

Applications of combinatorics

Combinatorics is applied in most of the areas such as:

- Communication networks, cryptography, and network security
- Computational molecular biology
- Computer architecture
- Scientific discovery
- Languages
- Pattern analysis
- Simulation
- Databases and data mining
- Homeland security
- Operations research

What are permutations and Combinations?

In English, we make use of the word "combination" without thinking if the order is important. Let's take a simple instance. The fruit salad is a combination of grapes, bananas, and apples. The order of fruits in the salad does not matter because it is the same fruit salad.

But let us assume that the combination of a key is 475. You need to take care of the order, since the other combinations like 457, 574, or others won't work. Only the combination of 4 – 7 – 5 can unlock.

Hence, to be precise;

- When the ***order does not have much impact***, it is said to be a ***combination.***
- When the ***order does have an impact***, it is said to be a ***permutation.***

Video: https://www.youtube.com/watch?time_continue=510&v=JyRKTesp6fQ&feature=emb_logo

Permutation: The act of an arranging all the members of a set into some order or sequence, or rearranging the ordered set, is called the process of permutation.

Definition

A permutation of r objects from a collection of n objects is any ordered arrangement of r distinct objects from the n objects.

- Notation: $(n)_r$ or ${}_nP_r$
- Formula: $(n)_r = \frac{n!}{(n-r)!}$

The special permutation rule states that anything permute itself is equivalent to itself factorial.

Example:

$$(3)_3 = \frac{3!}{(3-3)!} = \frac{3!}{0!} = 3! = 3 \times 2 \times 1 = 6$$

Note: Permutations of *n* items taken *r* at a time.

P (n, r) represents the number of permutations of *n* items *r* at a time.

$$P(n,r) = \frac{n!}{(n-r)!} = {}_{n}\mathrm{P}_{r}$$

I DO 1) P (7, 3)

YOU DO 1) P (15, 5)

WE DO 1) If a class has 28 students, how many different arrangements can 5 students give a presentation to the class?

EXTRA PROBLEM 1) How many ways can the letter of the word PHOENIX be arranged?

SPECIAL CASE OF PERMUTATIONS

Permutations with indistinguishable items

The number of different permutations of n objects, where there are n_1 indistinguishable items, n_2 indistinguishable items, ..., and n_k indistinguishable items , is

$$\frac{n!}{n_1!n_2!...n_k!}$$

I DO 1) How many ways can the letter of the word MATHEMATICS be arranged?

YOU DO 1) How many ways can the letter of the word COMMITTEE be arranged?

WE DO 1) How many ways can you order 3 blue marbles, 4 red marbles, and 5 green marbles? Marbles of the same color look identical.

EXTRA PROBLEM 1

A State's License plates consist of 3 letters followed by 4 digits. They will only allow you to choose from 18 letters and 9 numbers.

How many license plate options do they have if they CAN repeat letters and numbers?

How many license plate options do they have if they CANNOT repeat letters and numbers?

Question Help: Video

Video: https://www.youtube.com/watch?time_continue=6&v=SGn1913lOYM&feature=emb_logo

Combination: Selection of members of the set where the order is disregarded. ***The order does not MATTER!***

Combination

Definition

A combination of r objects from a collection of n objects is any unordered arrangement of r distinct objects from the n total objects.

Remark: The difference between a combination and a permutation is that order of the objects is not important for a combination.

- Notation: $\binom{n}{r}$ or ${}_nC_r$
- Formula: $\binom{n}{r} = \frac{n!}{(n-r)!\times r!}$

C (n, r) represents the number of permutations of n items r at a time.

$$C(n,r) = \frac{n!}{(n-r)!r!} = {}_{\mathrm{n}}\mathrm{C}_{\mathrm{r}}$$

I DO 1) C (7, 3)

YOU DO 1) C (15, 5)

WE DO 1) The soccer team has 20 players. There are always 11 players on the field at any one time. How many different groups of players can be on the field at any one time?

EXTRA PROBLEM 1) A student needs 8 more classes to complete her degree. If she has met the prerequisites for all the courses, how many ways can she take 4 classes next semester?

EXTRA PROBLEM 2) There are 4 men and 5 women in a small office. The customer wants a site visit from a group of 2 men and 2 women. How many different groups can be formed from the office?

EXTRA PROBLEM 3)

Lucy Furr must supply 3 different bags of chips for a party. She finds 18 varieties at her local grocer. How many different selections can she make?

Soruce: **https://www.mathplanet.com/education/pre-algebra/probability-and-statistics/probability-of-events**

Quick Lesson about Probability of Events

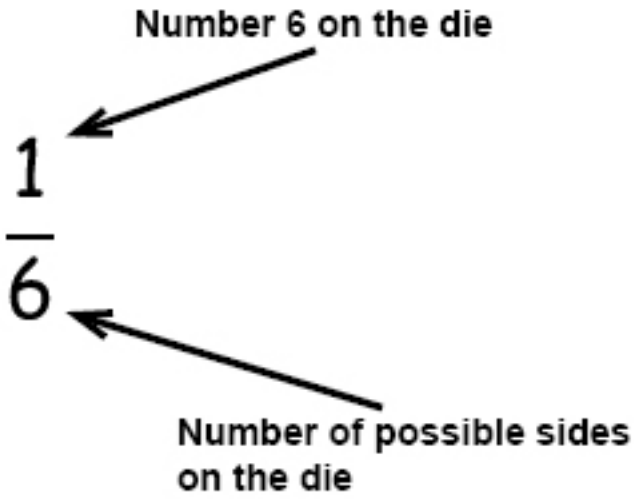
Probability is a type of ratio where we compare how many times an outcome can occur compared to all possible outcomes.

$$P(E) = \frac{favorable\ number\ of\ outcomes}{total\ number\ of\ outcomes}$$

Example 1:

What is the probability to get a 6 when you roll a die?

A die has 6 sides, 1 side contain the number 6 that give us 1 wanted outcome in 6 possible outcomes.



Independent events: Two events are independent when the outcome of the first event does not influence the outcome of the second event.

Note: ***When we determine the probability of two independent events, we multiply the probability of the first event by the probability of the second event.***

$$P(X \text{ and } Y) = P(X) \cdot P(Y)$$

To find the probability of an independent event we are using this rule:

Example

If one has three dice what is the probability of getting three 4s?

The probability of getting a 4 on one die is 1/6

The probability of getting 3 4s is:

$$P(4 \text{ and } 4 \text{ and } 4) = \frac{1}{6} \cdot \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{216}$$

Key Idea. When the outcome affects the second outcome, which is what we called dependent events.

Dependent events: Two events are dependent when the outcome of the first event influences the outcome of the second event. The probability of two dependent events is the product of the probability of X and the probability of Y **AFTER** X occurs.

$$P(X \text{ and } Y) = P(X) \cdot P(Y \text{ after } x)$$

Example. What is the probability for you to choose two red cards in a deck of cards?

A deck of cards has 26 black and 26 red cards. The probability of choosing a red card randomly is:

$$P(red) = \frac{26}{52} = \frac{1}{2}$$

The probability of choosing a second red card from the deck is now:

$$P(red) = \frac{25}{51}$$

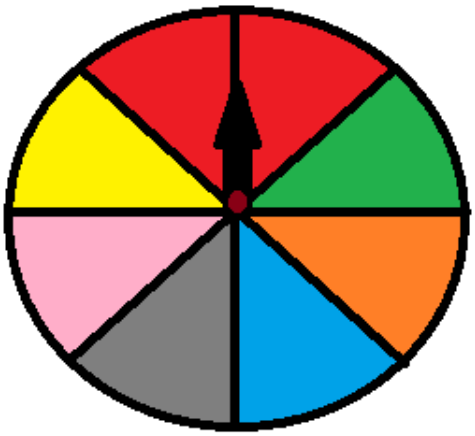
The probability:

$$P(2\ red) = \frac{1}{2} \cdot \frac{25}{51} = \frac{25}{102}$$

Key Idea. Two events are mutually exclusive when two events cannot happen at the same time. The probability that one of the mutually exclusive events occur is the sum of their individual probabilities.

$$P(X \text{ or } Y) = P(X) + P(Y)$$

Example: An example of two mutually exclusive events is a wheel of fortune. ***Let's say you win a bar of chocolate if you end up in a red or a pink field.***



What is the probability that the wheel stops at red or pink?

P (red or pink) = P(red) + P(pink)

$$P(red) = \frac{2}{8} = \frac{1}{4}$$

$$P(pink) = \frac{1}{8}$$

$$P(red\ or\ pink) = \frac{1}{8} + \frac{2}{8} = \frac{3}{8}$$

Key Idea. Inclusive events are events that can happen at the same time. To find the probability of an inclusive event we first add the probabilities of the individual events and then subtract the probability of the two events happening at the same time.

$$P(X\ or\ Y) = P(X) + P(Y) - P(X\ and\ Y)$$

Example

What is the probability of drawing a black card or a ten in a deck of cards?

There are 4 tens in a deck of cards P(10) = 4/52

There are 26 black cards P(black) = 26/52

There are 2 black tens P(black and 10) = 2/52

$$P(black\ or\ ten) = \frac{4}{52} + \frac{26}{52} - \frac{2}{52} = \frac{30}{52} - \frac{2}{52} = \frac{28}{52} = \frac{7}{13}$$

KEYWORDS:

With replacement means the same item can be chosen more than once.

Without replacement means **the same item cannot be selected more than once**.

Probability with permutations

$$\boldsymbol{P(E) = \frac{favorable\ number\ of\ outcomes}{total\ number\ of\ outcomes}}$$

$$= \frac{number\ of\ outcomes\ in\ event\ space}{number\ of\ outcomes\ in\ sample\ space} * 100\%$$

I DO 1: **You pick 3 digits (0-9) at random without replacement and write them in the order picked. What is the probability that you have written the first 3 digits of your phone number? Assume there are no repeats of digits in your phone number. Give your answer as a fraction.**

YOU DO 1) You pick 2 digits (0-9) at random without replacement and write them in the order picked.

What is the probability that you have written the first 2 digits of your phone number? Assume there are no repeats of digits in your phone number.

Give your answer as a fraction.

EXTRA EXAMPLE 1

Kosumi has 13 books and he wants to read 5 over the summer. He has 7 fiction books and 6 nonfiction books.

If Kosumi randomly selects the 5 books, what is the probability that the first 2 books are fiction and the next 3 books are nonfiction?

%

Question Help: Written Example

EXTRA EXAMPLE 2

Three cards are chosen without replacement from a deck of 52 cards and placed in order from first to third.

What is the probability that all three cards are spades?

[ ] %

Question Help: Video Written Example

Probability with combinations

$$\boldsymbol{P(E)} = \frac{\boldsymbol{favorable\ number\ of\ outcomes}}{\boldsymbol{total\ number\ of\ outcomes}}$$

$$= \frac{\boldsymbol{number\ of\ outcomes\ in\ event\ space}}{\boldsymbol{number\ of\ outcomes\ in\ sample\ space}} * 100\%$$

I DO 1) From a group of 12 people, you randomly select 4 of them. What is the **probability** that they are the 4 oldest people in the group?

YOU DO 1) From a group of 7 people, 2 are randomly selected. What is the probability the 2 oldest people in the group were selected? *Give your answer as a reduced fraction.*

EXTRA EXAMPLE 1

Combinations and Probability

An employee group requires 6 people be chosen for a committee from a group of 14 employees. Determine the following probabilities of randomly drawn committee of 6 employees.

Write your answers as percents rounded to 4 decimal places.

The employee group has 8 women and 6 men.

What is the probability that 4 of the people chosen for the committee are women and 2 people chosen for the committee are men?

[ ] %

The committee requires that exactly 2 people from IT serve on the committee. There are 5 people in IT.

What is the probability that exactly 2 of the people chosen for the committee are from IT?

[ ] %

Question Help: Video Written Example

QUICK REVIEW
QUESTION #1

Standard automobile license plates in a country display 3 numbers, followed by 2 letters, followed by 2 numbers. How many different standard plates are possible in this system? (Assume repetitions of letters and numbers are allowed.)

There are ____ different standard plates possible in this system.

Question Help: Video

QUESTION #2

3 -letter "words" are formed using the letters A, B, C, D, E, F, G. How many such words are possible for each of the following conditions?

(a) No condition is imposed.

There are ____ possible "words".

(b) No letter can be repeated in a word.

There are ____ possible "words".

(c) Each word must begin with the letter A.

There are ____ possible "words".

(d) The letter C must be at the end.

There are ____ possible "words".

(e) The second letter must be a vowel.

There are ____ possible "words".

Question Help: Video

QUESTION #3

An artist with a palette of 10 colors designs a flag with 3 different vertical stripes. Find the number of possible flags she can create.

QUESTION #4

A person going to a party was asked to bring 2 different bags of chips. Going to the store, she finds 17 varieties.

How many different selections can she make?

Question Help: Video

Source: https://www.cuemath.com/data/probability/
Probability of Dependent and Independent Events

Terminology of Probability Theory

The following terms in probability help in a better understanding of the concepts of probability.

Experiment: A trial or an operation conducted to produce an outcome is called an experiment.

Sample Space: All the possible outcomes of an experiment together constitute a sample space. For example, the sample space of tossing a coin is head and tail.

Favorable Outcome: An event that has produced the desired result or expected event is called a favorable outcome. For example, when we roll two dice, the possible/favorable outcomes of getting the sum of numbers on the two dice as 4 are (1,3), (2,2), and (3,1).

Trial: A trial denotes doing a random experiment.

Random Experiment: An experiment that has a well-defined set of outcomes is called a random experiment. For example, when we toss a coin, we know that we would get ahead or tail, but we are not sure which one will appear.

Event: The total number of outcomes of a random experiment is called an event.

Equally Likely Events: Events that have the same chances or probability of occurring are called equally likely events. The outcome of one event is independent of the other. For example, when we toss a coin, there are equal chances of getting a head or a tail.

Exhaustive Events: When the set of all outcomes of an experiment is equal to the sample space, we call it an exhaustive event.

Mutually Exclusive Events: Events that cannot happen simultaneously are called mutually exclusive events. For example, the climate can be either hot or cold. We cannot experience the same weather simultaneously.

Probability Formula

The probability formula defines the likelihood of the happening of an event. It is the ratio of favorable outcomes to the total favorable outcomes. The probability formula can be expressed as,

Probability Formula

cuemath
THE MATH EXPERT

$$P(A) = \frac{\text{Number of favorable outcomes to A}}{\text{Total number of possible outcomes}}$$

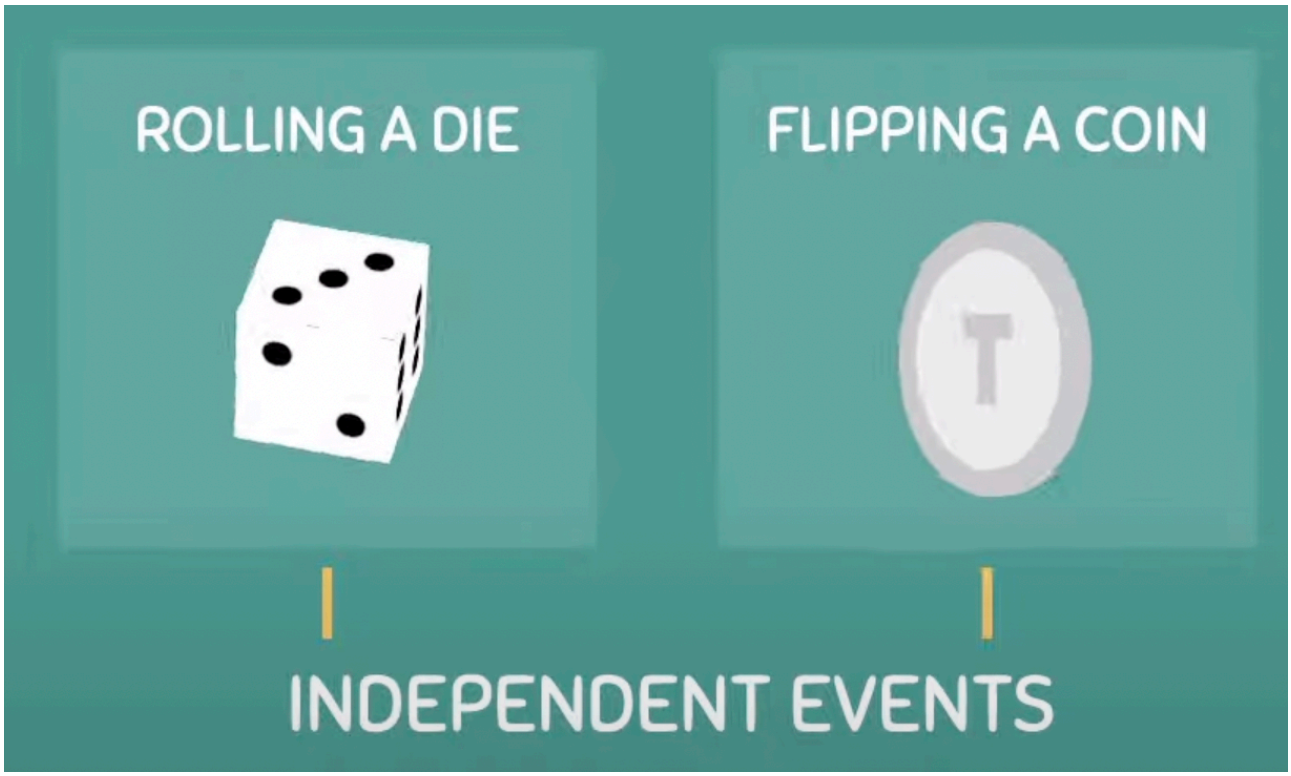
where,

- P(B) is the probability of an event 'B'.
- n(B) is the number of favorable outcomes of an event 'B'.
- n(S) is the total number of events occurring in a sample space.

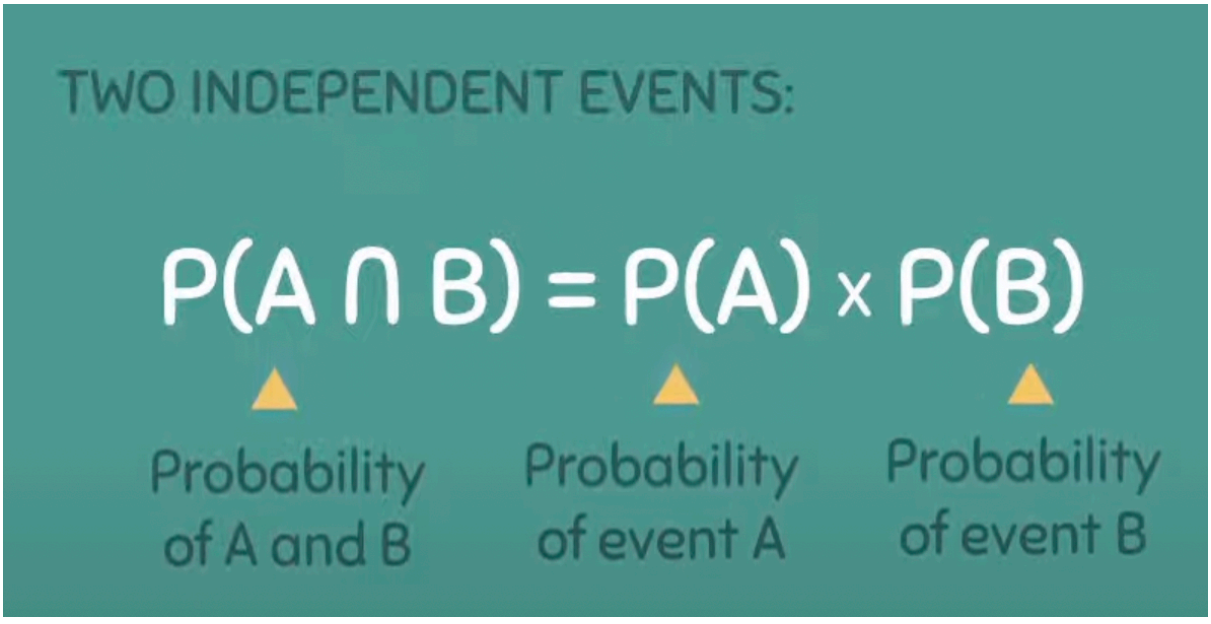
Video: https://www.youtube.com/watch?v=LS-_ihDKr2M

Dependent and Independent Events

For Example:



Formula:



EXAMPLE | If you roll a six-sided die and flip a coin, what is the probability of rolling a five and getting heads?

$$P(\text{Event}) = \frac{\text{total \# of favourable outcomes}}{\text{total \# of possible outcomes}}$$

$$P(\text{Rolling a 5}) = \frac{1}{6}$$

$$P(\text{Getting heads}) = \frac{1}{2}$$

$$P(A \cap B) = P(A) \times P(B)$$

$$= \frac{1}{6} \times \frac{1}{2}$$

$$= \frac{1}{12}$$

$$P(\text{Rolling a 5 and Getting heads}) = \frac{1}{12}$$

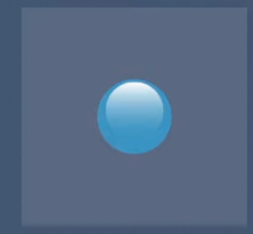
$$= 0.0833$$

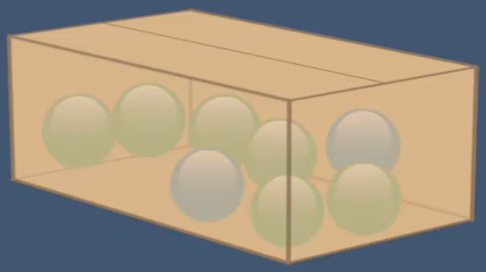
DEPENDENT EVENTS

Refer to the occurrence of one event affecting the probability of another event

EXAMPLE 1

P(Blue) = 3/10





P(Green) = 7/10

DEPENDENT EVENT

If we randomly select two marbles from this box, what is the probability of drawing a green marble and then a blue marble, without replacement?

$P(A \cap B) = P(A) \times P(B)$

$= 7/10 \times 3/9$

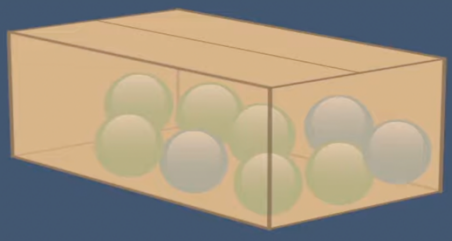
$= 7/30$

$= 0.233$

P(BLUE) = 3/9

P(GREEN) = 7/10

EXAMPLE 2



Event A = Drawing 1st Green Marble

Event B = Drawing 2nd Green Marble

DEPENDENT EVENT

What is the probability of drawing two green marbles without replacement?

$P(A \cap B) = P(A) \times P(B \text{ after } A)$

$= 7/10 \times 6/9$

$= 7/15$

$= 0.4667$

P(First Green) = 7/10

P(Second Green) = 6/9

WE DO 1

Alan places five white marbles and five black marbles into a bag. He then performs the two experiments described below to select two marbles from the bag.

First Experiment
One marble is selected from the bag and replaced before a second marble is selected.

Second Experiment
One marble is selected from the bag and not replaced before a second marble is selected.

The following two events are the same for each experiment:

Event X: The first marble selected is black.
Event Y: The second marble selected is white.

A) Which experiment is the dependent events?

B) Which experiment is the independent events?

WE DO 2

Mark Question for Use

A bag contains 8 $yellow$ marbles, 4 $green$ marbles, 7 $black$ marbles. If one marble is drawn from the bag then replaced, what is the probability of drawing a $yellow$ marble then a $black$ marble?

0.15512465373961

In a number guessing game. You ask a person to guess a number from one 1 to 10. If the person makes a random guess, what is the probability their guess will be less than 9?

0.8

A bag contains 4 $white$ marbles, 7 $black$ marbles, 8 $green$ marbles. If one marble is drawn from the bag but not replaced, what is the probability of drawing a $white$ marble then a $green$ marble?

0.093567251461988

Additional Different Probability Formulas

1) Probability formula with addition rule: Whenever an event is the union of two other events, say A and B, then
P (A or B) = P(A) + P(B) - P(A∩B)
P (A ∪ B) = P(A) + P(B) - P(A∩B)

2) Probability formula with the complementary rule: Whenever an event is the complement of another event, specifically, if A is an event, then
P (not A) = 1 - P(A) or P(A') = 1 - P(A).
P(A) + P(A′) = 1.

3) Probability formula with the conditional rule: When event A is already known to have occurred and the probability of event B is desired, then

P (B, given A) = P (A and B), P (A, given B).

It can be vice versa in the case of event B.
P(B|A) = P(A∩B)/P(A)

4) Probability formula with multiplication rule: Whenever an event is the intersection of two other events, that is, events A and B need to occur simultaneously. Then

P (A and B) = P(A)·P(B).

$P(A \cap B) = P(A) \cdot P(B|A)$

WE DO 3

Suppose that events A and B are dependent events with $P(A) = 0.35$, $P(B) = 0.26$, and $P(B \mid A) = 0.13$. Find the following probabilities and round your answers to 4 decimal places.

a. $P(A \text{ and } B) =$

b. $P(A \text{ or } B) =$

Suppose now that events A and B are independent events with $P(B) = 0.26$ and $P(A \mid B) = 0.14$. Find the following probabilities and round your answers to 4 decimal places.

a. $P(A) =$

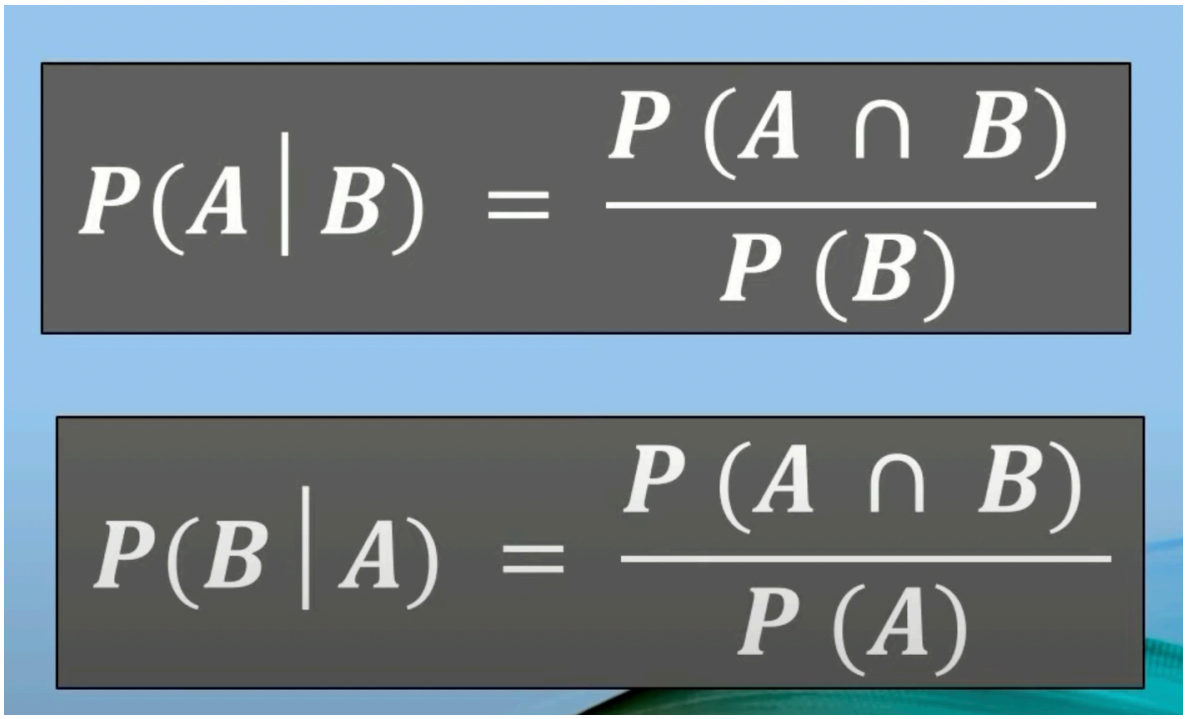
b. $P(B \mid A) =$

c. $P(A \text{ and } B) =$

Video: https://www.youtube.com/watch?v=kYfXpOJtRFc
Lecture: https://www.probabilitycourse.com/chapter1/1_4_0_conditional_probability.php#:~:text=If%20A%20and%20B%20are,P(B)%3E0.
Video: https://www.youtube.com/watch?v=r84YInEXMDo

Conditional Probability

And – multiplication (Union) or (addition) - Intersection



Here is the intuition behind the formula. When we know that B has occurred, every outcome that is outside B should be discarded. Thus, *our sample space is reduced to the set* B, Figure 1.21. Now the only way that A can happen is when the outcome belongs to the set $A \cap B$. We divide $P(A \cap B)$ by $P(B)$, so that the conditional probability of the new sample space becomes 1, i.e., $P(B|B) = \frac{P(B \cap B)}{P(B)} = 1$.

Note that conditional probability of $P(A|B)$ is undefined when $P(B) = 0$. That is okay because if $P(B) = 0$, it means that the event B never occurs so it does not make sense to talk about the probability of A given B.

It is important to note that conditional probability itself is a probability measure, so it satisfies probability axioms. In particular,

- Axiom 1: For any event A, $P(A|B) \geq 0$.
- Axiom 2: Conditional probability of B given B is 1, i.e., $P(B|B) = 1$.
- Axiom 3: If $A_1, A_2, A_3, \cdots$ are disjoint events, then $P(A_1 \cup A_2 \cup A_3 \cdots |B) = P(A_1|B) + P(A_2|B) + P(A_3|B) + \cdots$.

In fact, all rules that we have learned so far can be extended to conditional probability. For example, the formulas given in Example 1.10 can be rewritten:

Example 1.16
For three events, A, B, and C, with $P(C) > 0$, we have

- $P(A^c|C) = 1 - P(A|C)$;
- $P(\emptyset|C) = 0$;
- $P(A|C) \leq 1$;
- $P(A - B|C) = P(A|C) - P(A \cap B|C)$;
- $P(A \cup B|C) = P(A|C) + P(B|C) - P(A \cap B|C)$;
- if $A \subset B$ then $P(A|C) \leq P(B|C)$.

Let's look at some special cases of conditional probability:

- When A and B are disjoint: In this case $A \cap B = \emptyset$, so

$$\begin{aligned} P(A|B) &= \frac{P(A \cap B)}{P(B)} \\ &= \frac{P(\emptyset)}{P(B)} \\ &= 0. \end{aligned}$$

  This makes sense. In particular, since A and B are disjoint they cannot both occur at the same time. Thus, given that B has occurred, the probability of A must be zero.

- When B is a subset of A: If $B \subset A$, then whenever B happens, A also happens. Thus, given that B occurred, we expect that probability of A be one. In this case $A \cap B = B$, so

$$\begin{aligned} P(A|B) &= \frac{P(A \cap B)}{P(B)} \\ &= \frac{P(B)}{P(B)} \\ &= 1. \end{aligned}$$

- When A is a subset of B: In this case $A \cap B = A$, so

$$\begin{aligned} P(A|B) &= \frac{P(A \cap B)}{P(B)} \\ &= \frac{P(A)}{P(B)}. \end{aligned}$$

WE DO 1

Suppose a basketball team had a season of games with the following characteristics:

- 60% of all the games were *at-home* games. Denote this by *H* (the remaining were *away* games).
- 25% of all games were *wins*. Denote this by *W* (the remaining were *losses*).
- 20% of all games were at-home wins.

Of the at-home games, we are interested in finding what proportion were wins. In order to figure this out, we need to find:

- ○ P(H)
- ○ P(W)
- ○ P(H and W)
- ○ P(H | W)
- ○ P(W | H)

WE DO 2

Consider the data from a survey about preferred ice cream flavors:

	Chocolate	Strawberry	Total
Male	38	62	100
Female	56	44	100
Total	94	106	200

Based on the data, if we randomly choose a person, what is:

a. P(a person likes chocolate | male) _____

b. P(a person is female | they like chocolate) _____

WE DO 3

Giving a test to a group of students, the grades and gender are summarized below

	A	B	C	Total
Male	3	8	17	28
Female	15	10	2	27
Total	18	18	19	55

If one student is chosen at random,

Find the probability that the student was male GIVEN they got a 'B'.

WE DO 4

A home pregnancy test was given to women, then pregnancy was verified through blood tests. The following table shows the home pregnancy test results.

	Positive	Negative	Total
Pregnant	77	9	86
Not Pregnant	4	71	75
Total	81	80	161

Round your answers to the nearest thousandth.

$P(\text{positive} \mid \text{pregnant}) =$

$P(\text{pregnant} \mid \text{positive}) =$

$P(\text{negative} \mid \text{pregnant}) =$

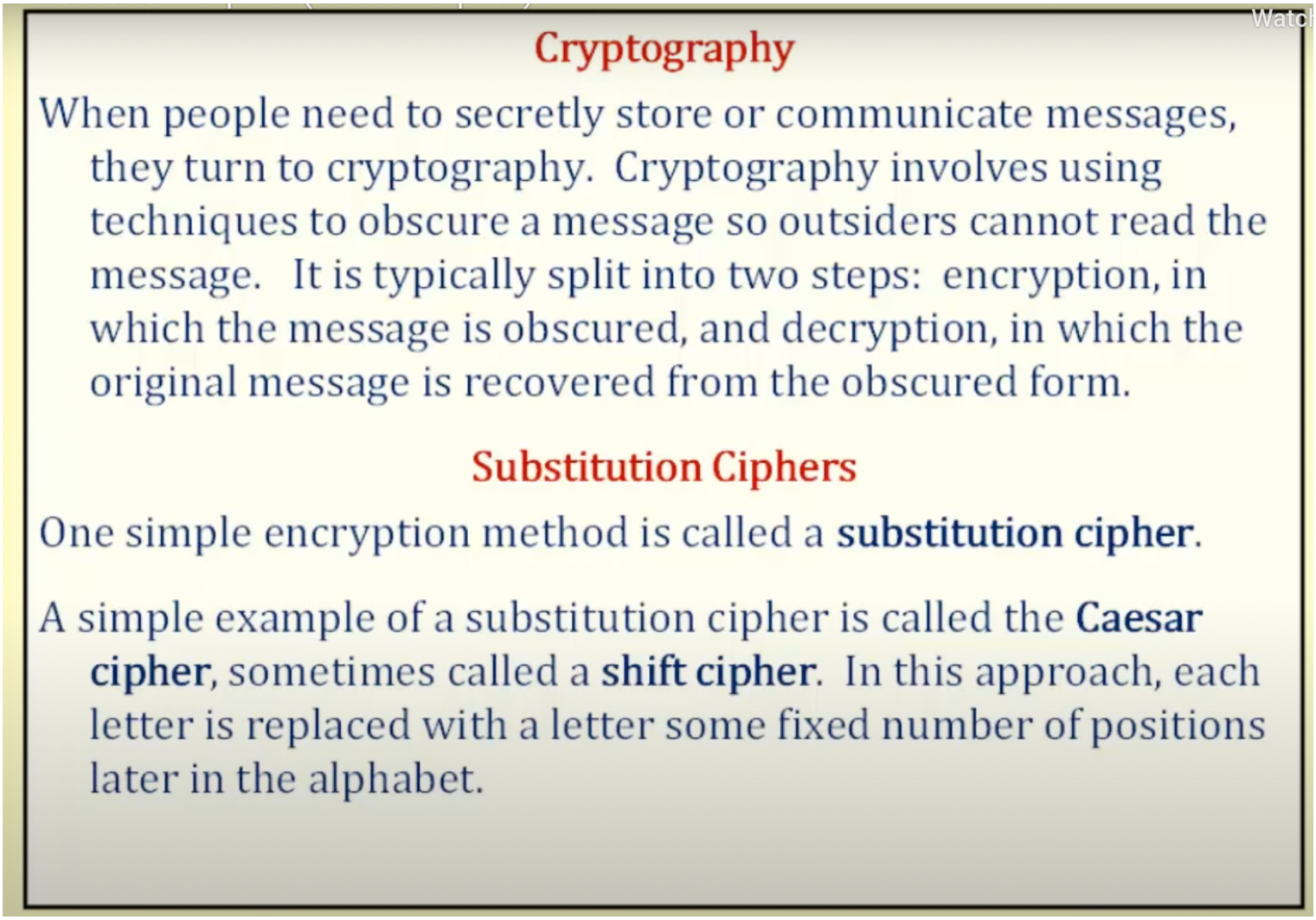
$P(\text{not pregnant} \mid \text{negative}) =$

Question Help: Video

Cryptography

Video: https://www.myopenmath.com/course/testquestion2.php?cid=158915&qsetid=31377&formn=selq&loc=qo0&checked=1

Cryptography and Encryption using Substitution Cipher



SAMPLE ENCRYPTION

Example: A Caesar cipher with a shift of 5 right would replace A with F, B with G, C with H, and so on.

A	B	C	D	E	F
A	B	C	D	E	F

Notice here after U is mapped to Z, we map the next letter V to A.

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps To	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Use the shift of 5 right to encrypt the following message. "Meet at the bank at eight AM" Write the final code in 4 letter blocks.

RJJY FYYM JGFS PFYJ NLMY FRAA

EXAMPLE DECRYPTION

Decrypt the word RPJHT if it was encrypted using an alphabetic Caesar shift cipher with shift 15 (mapping A to P).

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps To	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

CAUSE

Notice that in both the ciphers above, the extra part of the alphabet wraps around to the beginning. Because of this, a handy version of the shift cipher is a cipher disc, such as the Alberti cipher disk shown here from the 1400s. In a cipher disc, the inner wheel could be turned to change the cipher shift. This same approach is used for "secret decoder rings.

http://en.wikipedia.org/wiki/File:Alberti_cipher_disk.JPG

The security of a cryptographic method is very important to the person relying on their message being kept secret. The security depends on two factors:

1. The security of the method being used
2. The security of the encryption key used

In the case of a shift cipher, the **method** is "a shift cipher is used." The **encryption key** is the specific amount of shift used.

Suppose an army is using a shift cipher to send their messages, and one of their officers is captured by their enemy. It is likely the method and encryption key could become compromised. It is relatively hard to change encryption methods, but relatively easy to change encryption keys.

During World War II, the Germans' Enigma encryption machines were captured, but having details on the encryption method only slightly helped the Allies, since the encryption keys were still unknown and hard to discover. Ultimately, the security of a message cannot rely on the method being kept secret; it needs to rely on the key being kept secret.

Encryption Security

The security of any encryption method should depend only on the encryption key being difficult to discover. It is not safe to rely on the encryption method (algorithm) being kept secret.

Brute Force Attack

A brute force attack is a method for breaking encryption by trying all possible encryption keys.

Suppose you intercept a message, and you know the sender is using a Caesar cipher, but do not know the shift being used. The message begins **EQZP**. How hard would it be to decrypt this message?

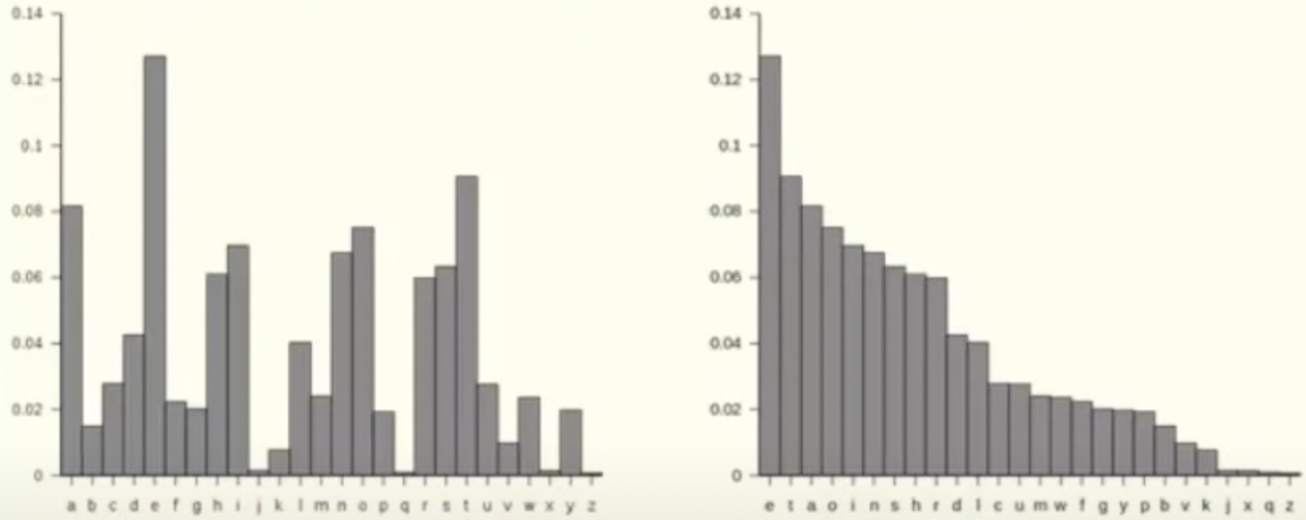
Since there are only 25 possible shifts, we would only have to try 25 different possibilities to see which one produces results that make sense. While that would be tedious, one person could easily do this by hand in a few minutes. A modern computer could try all possibilities in under a second.

Shift	Message	Shift	Message	Shift	Message	Shift	Message
1	DPYO	7	XJSI	13	RDMC	19	LXGW
2	COXN	8	WIRH	14	QCLB	20	KWFV
3	BNWM	9	VHQG	15	PBKA	21	JVEU
4	AMVL	10	UGPF	16	OAJZ	22	IUDT
5	ZLUK	11	TFOE	17	NZIY	23	HTCS
6	YKTJ	12	SEND	18	MYHX	24	GSBR
						25	FRAQ

To make a brute force attack harder, we could make a more complex substitution cipher by using something other than a shift of the alphabet. By choosing a random mapping, we could get a more secure cipher, with the tradeoff that the encryption key is harder to describe; the key would now be the entire mapping, rather than just the shift amount.

While there were only 25 possible shift cipher keys (35 if we had included numbers), there are about 10^{40} possible substitution ciphers. That's much more than a trillion trillions. It would be essentially impossible, even with supercomputers, to try every possible combination. Having a huge number of possible encryption keys is one important part of key security. There are 35 choices for what A maps to, then 34 choices for what B maps to, and so on, so the total number of possibilities is $35 \cdot 34 \cdot 33 \cdot \cdots \cdot 2 \cdot 1 = 35!$.

Unfortunately, this cipher is still not secure, because of a technique called frequency analysis, discovered by Arab mathematician Al-Kindi in the 9th century.



http://en.wikipedia.org/wiki/File:English_letter_frequency_(frequency).svg

WE DO 1) Write the shift of 7 right to encrypt the following message. “Hack the system at one PM”. Write the final code in 5 letter blocks.

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps to																										

WE DO 2) Decrypt the word NSCMBODO if it was encrypted using an alphabetic Caesar shift with shift 10 (mapping A to K)

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps to																										

EXTRA EXAMPLE 1

This question will guide you through the process of encrypting the sentence

the student stared at the quick airplane

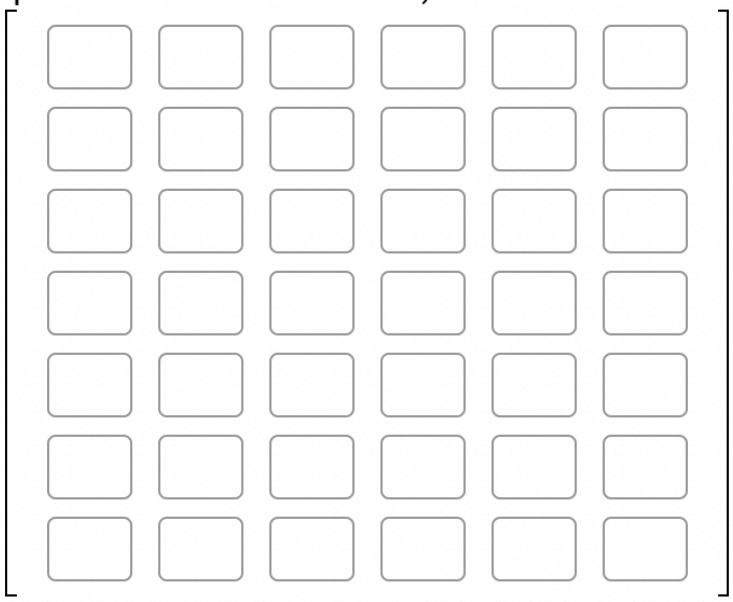
with the encoding matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 & 1 & 0 \\ 3 & -3 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Step 1

Replace each letter in the sentence with the corresponding number: a = 1, b = 2, etc. Use 0 for blank spaces. Enter your answer as a comma-separated list of numbers:

Step 2
Arrange your list of numbers into the following matrix, proceeding from left to right. If you have empty spots at the end of the matrix, fill them with zeroes.



Step 3
Multiply the matrix you created in step 2 with the encoding matrix: