Digital solutions Q&A

You added **encryption** to diagram or description. ALWAYS add a common-sense description like	The passenger data can be encrypted so that even if someone such as a hacker gains access to the passenger data files they cannot be read and used, hence securing the data.
Usability: User experience	**overall experience** of a person using a website or computer application, about how **easy or pleasing it is to use**
Usability: Usability principles	Accessibility, effectiveness, safety, utility and learnability
Usability: Usability principles [short]	accessible, effective, safe, useful, learnable
Usability: Usability principles [acronym]	"access safe effective useful learning OR Matt's version ..."
Usability: Usability principles [picture]	"Ute with safe in back, door open so you have access, a book on safecracking on top you used to learn. Because the safe is open, reading the book has been effective. OR Matt's version ..."
Usability: Can be used by many people, even people with disabilities	Accessibility
Usability: Users can use the system to do the work they need to do, including reliability	Effectiveness

Usability: Users can make errors and recover from the mistake	Safety
Usability: System easy to learn	Learnability
Usability: Accessibility	"Can be used by many people, even people with disabilities"
Usability: Effectiveness	"Users can use the system to do the work they need to do, including reliability What's the difference? Effective: Does what it is supposed to Utility: Does that more easily"
Usability: Safety	"Users can make errors and recover from the mistake"
Usability: Learnability	System easy to learn
Usability: HTML Semantic elements for screen reader or assistive device	"Accessible HTML Semantic elements are not visible for ordinary users, but when a user turns them on in settings, they will provide the type of output that user needs - for example big, clear text that tells someone with poor vision what an image is, or words that could be read out loud if the whole page is being read for someone without sight."
Usability: Terms of use confirms accessibility guidelines	Accessible
Usability: Search using Filter	Effective

Usability: Showing if account exists or is logged in	Effective
Usability: Quick links for frequently accessed info	Effective
Usability: Results per page selectable	Effective
Usability: Results current page 3 of 24	Effective
Usability: History backed up to cloud	Effective
Usability: Transaction log to trace false transactions	Effective
Usability: Error message in red plus how to fix	Safety
Usability: Padlock icon indicates secure access	Safety
Usability: List or grid view that might suit mobile or desktop	Utility
Usability: Descriptions	Utility

Usability: Metadata - date, time found etc	Utility
Usability: Consistent iconography through site to help first time users	Learnability
Usability: Online help accessible with interactive tutorials	Learnability
Usability: Support contact information	Learnability
In data flow diagrams, external entity is where	information enters or leaves the system.
In data flow diagrams, external entity may also be called	data source
In data flow diagrams, external entity might be (definition)	person organisation system that has predefined behaviour.
In data flow diagrams, external entity examples (one of each kind)	*person* - Jane, customer, student, client, user, teacher, staff member, manager, club member *organisation* - school, bank, business, university, IGS, club, department *system* that has predefined behaviour, often bits of code - start transation, end transaction, begin sort routine, end sort routine
In data flow diagrams, if something in the system cannot be	external entity.

changed by the system, it is called	
In data flow diagrams, a process first	changes data
In data flow diagrams, a process changes data then	produces output.
In data flow diagrams, give three examples of processes	Calculate, Sort, Direct, Print, Scan, Update, Pay, Login, Search, Generate, View, ... Print receipt, Scan membership card, Update user details, Pay subscription, Login, Search teacher, Generate movie report, View customer photos ...
In data flow diagrams, a process has how many inputs	at least one
In data flow diagrams, a process has how many outputs	at least one
In data flow diagrams, what is a data store	repository or file
In data flow diagrams, if the datastore is a permanent computer file, the datastore letter is	D (disk or database)
In data flow diagrams, if the datastore is a a manual file, the datastore letter is	M (manual)

In data flow diagrams, give an example of a manual store	pile of forms in-tray people in a queue cars in a queue ...
In data flow diagrams, a computer database would be which element	datastore
In data flow diagrams, a computer database would have which datastore element	D (disk or database)
In data flow diagrams, a transient datastore (T datastore) example might be	temporary disk file that will not be kept a desk where forms are sorted dash-cam memory which is continuously overwritten with new video when its memory limit is reached ...
In data flow diagrams, if the datastore is transient, the datastore letter is	T (temporary = transient)
Context diagrams have how many processes?	one (usually a circle)
The label on the single process in a context diagram usually starts with	what the system is about eg: Ebay customer
The label on the single process in a context diagram usually ends with	information system eg: Ebay customer information system

In context and data flow diagrams, flow from one symbol to another has two parts	- an arrow showing which way the information flows - labels which say what the information is
In data flow diagrams, when analysing the key words first look for	"external entities Things that will not be changed by the system: Customer, Bank, ATM, buoy, aeroplane, car, engine (all nouns)"
In data flow diagrams, when analysing the key words and you have found the external entities, next identify	"the processes (something that will be done in the system (a verb)) Print, Scan, Update, Pay, Login, Search, Generate, View, ... Add to the process labels what is being done: Print receipt, Scan membership card, Update user details, Pay subscription, Login, Search teacher, Generate movie report, View customer photos ..."
In data flow diagrams, when analysing the key words and you have the external entities and processes, finally find	"the datastores Doesn't have to be last, but on your sketch it may be handy to put them near the processes that need them (Customer database near 'Scan membership card', and so on."
In data flow diagrams, when analysing the key words and you have found the external entities, processes, datastores	- Ignore anything not stated in the problem! - check your three lists against the problem to see you have everything in one of the lists.
"Sue connected her IGGS account. A message box popped up asking if she wanted to chat with with her teacher, Ms May. She clicked OK, and she was joined to the meeting.	Draw your own. Sue connected her IGGS account. A message box popped up asking if she wanted to chat with with her teacher, Ms May. She clicked OK, and she was joined to the meeting. Draw the **concept** diagram.

Draw the **concept** diagram."

"Sue logged into her IGGS account. A message box popped up asking if she wanted to join a zoom meeting with with her teacher, Ms May and other students. She clicked OK, and she was joined to the meeting.

If you know the school's computer handles all this, what are the external entities?

What are the processes?

What are the datastores?

Draw the **data flow** diagram.

Ms May has to login too. Ms May's login details are in the teachers database, while Sue's login details are in the student database. Add these to your data flow diagram."

"Draw your own.
Sue logged into her IGGS account. A message box popped up asking if she wanted to join a zoom meeting with with her teacher, Ms May and other students. She clicked OK, and she was joined to the meeting.

If you know the school's computer handles all this, what are the external entities?

What are the processes?

What are the datastores?

Draw the **data flow** diagram.

Ms May has to login too. Ms May's login details are in the teachers database, while Sue's login details are in the student database. Add these to your data flow diagram."

"What is the basic problem of these pages in the same app?
"

They are not consistent

"You are asked to comment on the background colour of

1. The problem is that all the pages have different background colours.
2. This may confuse users because they may not realise when they move from one page to another they are still on the same site.

these pages from the same app. 1. Say what the problem is. 2. Say why it is a problem. 3. Say how it could be fixed. 4. Give the benefits of your fix. "	3. The fix is to make all the pages have the same background colour. 4. Then users would realise in moving from page to page that they are still on the same site.

"You are asked to comment on the background colour of the navigation bars in these pages from the same app. Say what the problem is. Say why it is a problem. Say how it could be fixed. Give the benefits of your fix. "	The problem is that the navigation bars have several different background colours. This may confuse users because they may not find the navigation bar easily when they move from one page to another they are still on the same site. The fix is to make all the navigation bars have the same background colour. Then users would easily find the navigagion bars in moving from page to page.

Usability: Utility	"Utility functions are things that help the user get the job done. What's the difference? Effective: Does what it is supposed to Utility: Does that more easily"

A library search app returns 1,200 titles in one long list. Which are not true: 1. The app is effective 2. The app is useful 3. The app is accessible 4. The app is safe	"1. The app is effective - it does what it has to - finds the books that meet the search criteria. 2. The app is useful - **No.** Scrolling through 1,200 titles could take forever. 3. The app is accessible - We can't say anything about that. 4. The app is safe - We can't say anything about that."

"Our book search app returns 1,200 finds in one long list on one	"Jim's opinion: Filter option on the search: Perhaps make list much smaller. Results per page selectable: Less information to handle at a time.

screen. It is effective. It is not useful What are some things that might improve this page's utility? and how?"	Font size display button: User can see more easily, or fit more in, depending on eyesight. A current page box eg: 'Page 3 of 123': User can see how far they have got through. List/Grid view so it suits mobile/desktop: Useful whichever device the user is using at the time."
Safety Give five features that improve safety. Give the reason they protect the user from any mistake or omission they may make.	"Error message in red plus how to fix: The mistake or omission won't kill the activity and the user can see how to fix it. Padlock icon shows secure access: User can trust that information will come to/from the site without strangers inbetween being able to see it. Breadcrumb trail: User can see where they are, and click to return to a higher level. History backed up to cloud: If this device is dead, the data will still be available. Transaction log: User can see improper activity and take steps to fix."
"What's wrong about using this to choose a language? And what would be better? "	"Languages aren't countries and flags aren't countries. Using the British flag may offend people in other countries who speak English, an so on. Don't offend people unnecessarily. Instead, perhaps use one of the international icons for choosing languages: "
"This clever animation rolls up your receipt and whisks it away. That takes 3.5 seconds. Is there anything wrong with that? "	"A fade would take 0.25 seconds, and not waste user time. Making clever animations makes the creator feel warm and fuzzy, but not the user, especially after the novelty wears off. After you have entered your code, the animation below zips up in 0.5 seconds "
"Comment from a user interface aspect: "	"Firefox was mostly written by people who speak English. So, they probably is a link to change languages here. But only if you speak Chinese. If a site has more than one language version, there should be a clear way to change the language on every page. Perhaps the international icon: "
"How might this UI be improved?"	"Very long dropdowns are not good because they take time. A completion box where you begin to type, which narrows your

	choice Maps are no good for small countries. Perhaps organize by Region: "
"Comment"	"Some services make it hard for users to make choices (like NOT joining a mailing list, or NOT paying for flight insurance) by hiding the choices. Users end up harbouring hard feelings towards such services. Make all user choices clear. "
"The phone is on the left, the desktop version is on the left. Comment. "	"A website should be responsive. It should respond to the shape and power of the device it is showing on, like this app: "
" Comment"	"User is boss! Make it easy for them. As a bonus, you might get free exposure on Facebook or Twitter if one of those is chosen. "
"This Canadian airline site won't let me enter my mobile number so I can be reached in Australia: "	"We Australians are annoyed to have to remember the 202-456-1414 phone number and the 90210 zip code just so we can complete forms (even though we don't live in the White House or Beverly Hills). Don't make things difficult for users who aren't just like you. Make data entry as accepting as possible."
"Comment"	"Too much information. Poorly organised. This is better because the days are clear, the hours are clear, and colour makes the free time clear. "
" Comment"	"1. Do you really need this information? 'First name/Last name' or even just 'Your name' generally suits most people today. 2. Titles raise issues of gender identity. Don't make people feel uncomfortable unnecessarily."
" Comment on this old	"Not simple - cluttered, no clear organization, no use of shades of colour to make important stand out from unimportant, unlike the new,

iTunes interface"	which does use colour, organization, common Apple icons: "
" Comment"	"To get rid of this modal box (popup window), you have to admit that you don't appreciate good food. Annoying potential customers is never a good idea."
" Comment"	"On a main menu, 'About us' might be one of the things someone would expect. The rest of that submenu would be unlikely to be of much interest to visitors The fix would be to make a single 'About us' on the home page, and on the About us page have Values, Mission and endorsements on the navigation at the top of that page, or simply make them available by scrolling the About us page."
" On this home page of a travel company, you are shown a video of a diver, and you are not allowed to proceed until you click AND hold the button. Comment"	"The video will be slow to load on some devices - adding an annoyance to the user. The 'clever' video should be replaced. In general, animation and videos should not get in the way. The user has no clue if they have arrived on the site they are after. There should be a major indication on the home screen who offers the site. The user has no idea what will happen if they do click and hold. On a home page, what is where should be clear, and certainly all the clickable elements should be much like the user would expect on most home pages. The animation on this page below (an owl that blinks when you scroll over it) is both clever, not in the way and fits into the company's image There is a good use of space, and the indicator at the bottom of the page tells users the next expected action is for them to go downwards. "
(SQL) make a database for frogs	(SQL) CREATE DATABASE frogs;
(SQL) We have a database called hats. That was wrong. We should rub it out.	(SQL) DROP DATABASE hats;

(SQL) You already have created a database about pets. Now create a table in the database for owners

CREATE TABLE owners;

"(SQL) You already have created a database about horses. Now create a table in the database for owners that has the owner's name, address, horse, description, number of foals."

"CREATE TABLE owners (name, address, horse, description, foals);
== OR this is the same thing spread out with more space:
CREATE TABLE owners (
    name,
    address,
    horse,
    description,
    foals
);
Any word for table names (except words in SQL like CREATE, DROP ...)"

"(SQL) You already have created a database about horses. Now create a table in the database for owners that has the owner's name, address, horse, description, number of foals.
This time with appropriate field types."

"CREATE TABLE owners (
    Name varchar(100), -- the length is anything you choose up to 255. 255 is common
    Address varchar(100),
    Horse varchar (100),
    Description text,
    Foals int
);
int (short for integer) is most commonly used for integer numbers.
varchar (short for **var**iable number of **char**acters) Is most commonly used for words
varchar(255) a field for words up to 255 characters long is very common
text most commonly used for fields with words that might be very short or very long"

(SQL) We have a table in our database called men. That was wrong we should rub out that table.

(SQL) DROP TABLE men

"CREATE TABLE owners (
    name varchar(100),
    address

address varchar(255),

varchar(100),
    horse varchar(100),
    description text,
    foals int
);
The address needs to be 255 characters long.
One of the lines in this code needs to be fixed.
Give the fixed line."

(SQL) in a CREATE TABLE statement, how do you make a field for Title up to 50 characters long?

(SQL) Title varchar (50),

"(SQL) Create a table called student that has two fields – name, age with field types"

"(SQL) CREATE TABLE student (Name varchar(255) , Age int);"

(SQL) CREATE TABLE student (Name, Address , Age);
When you make more white space for this statement, what are the two punctuation mistakes easy to make?

"CREATE TABLE student
(
    Name,
    Address,
    Age   -- adding an unnecessary comma after the last field
);   -- forgetting the semicolon that finishes every statement"

"(SQL) My student table has three columns name, address and phone.
I want to remove the phone number column and add a parent column.
What are the commands?
Extra marks if you can add a paid column that can only be true or false"

ALTER table student
DROP COLUMN phone;

ALTER table student
ADD COLUMN paid BOOLEAN;

"(SQL) My student table has two columns - name and address. I want to add a parent column. What are the commands?"	"ALTER TABLE students ADD parent varchar(255); = the width of the parent column could be any sensible number, but 255 is commonly used for efficiency = any text type field could have been used instead of varchar() here - **char(25)** if there was not much to say, **text** if there could be loads added. Notice there is no column size for the text column because it's size can range from 1 to massive."
SELECT * FROM Customers;	Get every single record from the customer base.
Most inefficient command in SQL	SELECT *
"SELECT * FROM dogs WHERE dogsName = 'fido';"	get all the mutts named fido from the dogs table
SELECT * FROM dogs WHERE dogsAge < 3;	get puppies from the dogs table
SELECT * FROM patients WHERE immunised = TRUE;	which people in the patients table have been immunised?
Say in approximate English: SELECT * FROM students WHERE age > 12 and age < 20;	Write in SQL Pick all the records in the students table whose age is more than 12 and less than 20.
"What is wrong with this SQL.	"There is an extra ; breaking the line in two. The first line will return all of the records in the table.

SELECT * FROM Customers; WHERE CustomerID=1;"	The second broken line return an error, because WHERE in a command can only follow SELECT, UPDATE, DELETE etc."

"SELECT *age*, *interests*, ... FROM *members* WHERE *suburb* = *'Kenmore'*;"	"From the members table, show me the age and interests of everyone in Kenmore"

"SELECT *age, pets* FROM *family* INNER JOIN *neighbours* ON *family.income = neighbours.income*;"	"Make a table of age and pets columns where there are people with the same income in both the family and neighbours tables. "

"SELECT Orders.OrderID, Customers.CustomerName, Shippers.ShipperName FROM ((Orders INNER JOIN Customers ON Orders.CustomerID = Customers.CustomerID) INNER JOIN Shippers ON Orders.ShipperID = Shippers.ShipperID); What is the result in English"	We have three tables, in order going down SELECT Orders.OrderID, Customers.CustomerName, Shippers.ShipperName FROM ((Orders INNER JOIN Customers ON Orders.CustomerID = Customers.CustomerID) INNER JOIN Shippers ON Orders.ShipperID = Shippers.ShipperID); So, we are going pick only those things that are in **both** Orders and Customers first, when you look a CustomerID in both. Then we are going to see what is in that set and also in Shippers, when you look at ShipperID in both. Finally we look to the top line Orders.OrderID, Customers.CustomerName, Shippers.ShipperName and see that we have to pick out the orderID from Orders, the CustomerName from Customers, and the ShipperName from Shippers. **Plain English:** we are picking out orders, customers, and shippers where we can match the records for all three. The first INNER JOIN leaves us with just the redish intersection: The second INNER JOIN leaves us with just the dark green intersection of all three orders: "

What is latency?	"Period of time delay from when data is requested to when it is received."

"What do we call the time data takes to reach its destination across network?"	latency (called lag by gamers)
What are high and low latency?	"low latency= very little delays (fast transmission time), high latency= lots of delays (slow transmission time)."
Factors effecting latency	"- serialisation - propagation - switching - queuing"
"serialisation"	"time it requires to assemble and transmit a data packet"
propagation	"time it takes for a signal to get from one place to another"
switching	"switch inspects data packets and redirects to appropriate browser → additional delays"
queueing	"data waits in queue for transmission to systematically manage traffic when network link is busy "
"When data buffers and data collisions cause additional delays that is part of ..."	queueing (which is part of latency) so either answer
jitter	"variation of latency over time"
high jitter	"data packet delivery time is very inconsistent"

no jitter	"every information packet takes same time to travel from A to B"
"Identify the (4) network transmission principles"	latency, jitter, timeliness, Quality Of Service guarantee
timeliness	time between when data is expected to arrive and when it does arrive
"delivering data as they are produced in the same order that they are produced without significant delay is"	timeliness
QOS guarantee ... Quality Of Service guarantee	giving a data flow priority eg guaranteeing that on your connection Netflix will always get through no matter what
managing data queueing and bandwidth so one particular service will almost always get through first is:	QOS guarantee or Quality of service guarantee
Data encrypted, sent over the network, decrypted at the other end, so no one inbetween can understand the data	VPN (virtual private network)
rules governing the exchange of different types of files that make up web pages	HTTP (HyperText Transfer Protocol)

FTP (File Transfer Protocol)	rules for transfer of files on Internet Commonly used when downloading program files.
Internet protocol which guarantees secure transmission	HTTPS
a set of rules	protocol
human readable protocols for data interchange	XML, JSON, REST
JSON is an abbreviation for	JavaScript Object Notation
Data Encryption Standard abbreviation	DES
A protocol in the TCP/IP suite that transports information over the Internet for access by Web browsers.	HTTP Hypertext transfer protocol
Allowed the creation of the world Wide Web and allowed users to send documents and images across networks.	HTTP
the capacity of a particular transmission	bandwidth

medium to move data is called its	

---

a group of two or more devices/computers connected together to allow for the exchange and information and for the sharing of resources such as printers	network

---

SQL command to erase a whole system is **DROP DATABASE**	Example: DROP DATABASE igaStores;

SQL command to start a new system is **CREATE DATABASE**	Example: CREATE DATABASE igs;

SQL command to start a new table is **CREATE TABLE**	"Example: CREATE TABLE students (studentID int, *name varchar(255)*, *address varchar(255)*, *age int*);"

SQL command to erase a whole table completely forever is **DROP TABLE**	"Example: DROP TABLE *hobbies*;"

SQL command to add or delete whole tables in a database **ALTER**	"Examples: ALTER TABLE Friends ADD Email varchar(255); ALTER TABLE Customers DROP COLUMN Email;"

SQL command to add a new row to an existing table is **INSERT INTO** **VALUES**	"Examples: INSERT INTO *dogs* (*name*, *age*) VALUES ('*Spot*', *12*); "

SQL command to change some of the existing records in a table **UPDATE** **SET** **WHERE**	"Example: UPDATE Customers SET ContactName = 'Simon Ng', City= 'Sydney' WHERE CustomerID = 1;"

SQL command to choose some records **SELECT**	"Example: SELECT CustomerName, City FROM Customers;"

"SQL command to select every record in a table is **SELECT * FROM**	"Example: SELECT * FROM Customers;"

"

SQL
modifier to specify
particular columns and
particular rows

WHERE

"Example:

SELECT stagename hometown FROM movieStars
WHERE Country='USA' AND age > 70;"

SQL
Which modifier picks
certain records

WHERE

"Example:

SELECT * FROM fireWardens
WHERE age > 70;
"

"SQL
command to sort the
selection into
alphabetical order or
numberical order

ORDER BY ASC

**Leave out ASC? Fine.
It works this way
anyway.**

"

"Explanation:

ASC is short for ascending - starting at the lowest and going up.
Letter A, B, ... or number 0, 1, 2....

Example:

SELECT * FROM students
WHERE studentName BETWEEN 'Mary' AND 'Oliver'
ORDER BY studentName ASC;

Puts in alphabetical order - Mary at the top, Oliver at the bottom"

SQL
command to sort the
selection into
REVERSE alphabetical
or numberical order

ORDER BY DESC

"Explanation:

DESC is short for descending - starting at the highest and going down.
Letter Z, Y, X ... or number 999, 998, 997 .

Example:

SELECT * FROM students
WHERE studentName BETWEEN 'Mary' AND 'Oliver'
ORDER BY studentName DESC;

Puts in reverse alphabetical order - Oliver at the top, Mary at the
bottom"

SQL modifier to count how many in each category **GROUP BY**	Example: SELECT Country FROM Customers GROUP BY Country;

SQL modifier to sort **ORDER BY**	Example: SELECT Country FROM Customers ORDER BY Country;

SQL Looking for something that is in both tables **INNER JOIN**	"Example: Inventions INNER JOIN ozProducts picks only things that are in both tables"

SQL The best data type for character strings of variable length, and well defined upper limit, use **varchar**	Example: firstName vchar(25)

SQL The best data type for character strings of fixed length, use **char**	Example: ipAddress char(15)

SQL The best data type for character strings with little control of the	Example: myReview text

length, use

TEXT

SQL
HAVING and ON both do the same as

WHERE

That is all you need to know to understand SQL queries.

Example:

All three pick student numbers higher than 100:
WHERE studentNo > 100
HAVING studentNo > 100
ON studentNo > 100

Only coders need to know where to use each one.

SQL
Nesting - one SQL query inside another. You evaluate the

inside query first

"Example:

```
SELECT age
FROM dogs
WHERE age > (SELECT AVG(age)FROM dogs);

Do the inside query first.
If the average age of dogs was, say, 8,
the outside query is then done using that:

SELECT age
FROM dogs
WHERE age > (8);


"
```

Encryption
The sentence you are given to encrypt is called

Plaintext

Encryption
The output of an encryption system is called

Ciphertext

Cipertext can be sent safely.
Ciphertext can only be decrypted with the same encryption system and same key.

Encryption
An encryption system is often public, but the special code that is private only to the sender and reciever is called a

private key

Encryption
In Vigenère square the private key known only to both ends is

keyword

Encryption
In the Vigenère square encryption system, the key is made by adding the keyword to itself until

it is the same length as the plaintext

Example

Keyword HAM
Plaintext FROGHASALEG
Key HAMHAMHAMH

or

Plaintext FROGH ASALE G
Key HAMHA MHAM H

"Encryption
In the Vigenère

Keyword: SIMON

What is the key for Plaintext: FROGH ASALE G
and what is the first letter of the ciphertext?

"

"Keyword: SIMON
Plaintext: FROGHASALEG
Key: SIMONSIMONS
so the first letter of the ciphertext is in row F and column S
Ciphertext: X

"

"A poly-alphabetic cipher uses

two or more alphabets written under each other or beside each other

"

Simplest poly-alphabetic cipher uses two alphabets. It is

Caesar cipher

"Example:
Caesar cipher has two alphabets.
One is shifted so the two do not match. Leftover letters are added to the front
The second alphabet below has been shifted 3 places to the left.
"

A poly-alphabetic cipher that uses twenty-six alphabets is

Vigenère square.

"Example:
In the Vigenère square (or Vigenère table) each next alphabet is shifted one place.
"

The Gronsfeld cipher works the same as the Vigenère cipher except the rows are labelled by

numbers

""

Vigenère cipher: table has the alphabet repeated 26 times.
Gronsfeld cipher: table has the alphabet repeated

any number of times

"usually 9 or less rows,
usually with 9 or less columns
like this one:

"

"A Cipher that uses more than one alphabet is called a

"Explanation:

poly = many

Polyalphabetic cipher

"

eg polytechnic college = one that teaches many technologies

so polyalphabetic = many alphabets"

Three rules that are often used on sentences to be sent as cybertext through the public are:

Remove spaces and punctuation
Make all caps
Put in groups of 5

Example:
Three rules that are often used on sentences to be sent:

1. Threerulesthatareoftenusedonsentencestobesent

2. THREERULESTHATAREOFTENUSEDONSENTENCESTOBESENT

3. THREE RULES THATA REOFT ENUSE DONSE NTENC ESTOB ESENT

Cryptographers working on paper usually leave them in these groups while they do their work.

Only one encryption method has been proven to be unbreakable

one time pad

Explanation:

It is only unbreakable if you completely follow all the rules.

"Symmetric encryption systems are ones where the

same key can be used or encryption at one end and decryption at the other

"

"with a key, you can:

encript plaintext to ciphertext, or
decrypt cyphertext to plaintext.

Symmetric = balanced = same key both ends"

Asymmetric encryption systems have two keys:

public key
private key

Examples:
The banking app on your phone has the
public key (bank)
private key (yours) which you have previously shared with the bank

Asymmetric = NOT balanced = different keys both ends

"SQL
In my doctor's medical system, you can only put in the Medicare number with exactly 11 digits.

The datatype and length for the Medicare number column in his system is probably

char(11)

"

"Explanation:

Any character field, including char, varchar and text would work, but only char would be efficient
for data whose exact length is known."

"The cryptography part of a public key system ensures that any message
encrypted with Bob's **public** key
can only be decrypted

by Bob's private key

"

I click on youtube.com in my browser.
The message gets to youtube.
Youtube sends a back a certificate.
My browser is looking for two things in this certificate

**signature from a trusted Certificate Authority (like Google CA) and
a public key from youtube.com**

"A website sent your browser a certificate signed by the Google CA.
To check that the certificate was really signed by the Google CA, your browser will need to have

Google CA's public key.

"

"Explanation:

If you have Bob's public key, you can check that something that says it came from Bob, really came from Bob."

"**Not yet ready**
Your bowser gets a certificate from Netflix signed by Google CA, gets the public key of Google CA,
uses this Google CA public key to check that the certificate was really signed by Google CA,
then your browser creates you a new private key using the Netflix public key that was in the certificate and sends your new private key to Netflix.
Because it was prepared using the Netflix public key, Netflix knows it is the only party that can decrypt your message, so now both you and Netflix have the **same private key** you both can use to encrypt messages both ways."

not yet ready

Scrambling data so that only the desired party can understand that information is

encryption

Scrambling data so that it cannot be unscrambled (encrypting data so it cannot be decrypted) is

hashing

"The individual code made is a hash. Hashes are stored in a hash file."

"Facebook friends: encrypted or hashed before it is stored?

encrypted

"

Facebook wants to look up the friends for all sorts of reasons, so it is encrypted

---

"Facebook password: encrypted or hashed before it is stored?

hashed

"

"Explanation:

hash - same password → same hash → can be checked every time it is entered.
hash - can't be reversed. Can't find someone's password from their hash"

Symmetric encryption systems have how many keys?

one - the secret key

secret key also called shared key

In a hash file, the length of every hash is

the same

"ChaCha20 and Salsa20 are stream ciphers.
They encrypt the digits or letters

one at a time
"

AES is a block cipher.
AES organizes the plaintext into

blocks

AES uses 128-bit blocks

AES uses 128-bit blocks
If the plaintext is shorter than 128 bits, before it is encrypted:

dummy plaintext is added to the end to make it 128 bits long

Plaintext 128 bits long → 1 block
Plaintext 256 bits long → 2 blocks

Plaintext 28 bits long → 28 plaintext bits + 100 dummy bits → 1 block

---

"Symmetric = balanced = same key both ends
Name some symmetric encryption systems

Blowfish,
Twofish,
DES (Data Encryption Standard),
3DES (Triple DES),
RSA (Rivest–Shamir–Adleman)
AES (Advanced Encryption Standard)
FPE (Format Preserving Encryption)

also Vigenère, Grosfeld, Caesar, one time pads are older and not currently used (except one time pads in diplomatic communication)

"

"You have a single key.

You can both:
encript plaintext to ciphertext,
or
decrypt cyphertext to plaintext.
at both ends.

Your encryption system
is

symmetric

"

One encryption method
used in modern desktop
and laptop computers
because the CPU has a
special section that
speeds it up.
It is

**AES (Advanced
Encryption Standard)**

AES (Advanced
Encryption Standard)
encryption method is
used in modern desktop
and laptop computers
because the CPU has a
special section that
speeds it up.

Mobile devices often
do not have this CPU

So, they use
ChaCha20 to encrypt
because it is small, fast

and secure.

In my amateur system, when users log on:
counts the number of letters in their password
stores that number with their name in a file.

This is a simple **hash** table.
Would it work as a **hash**?
1. Explain why.

2. Say why it might be insecure.

3. Say how you might improve the system

"1.
A hash function must:
- give the same result for the same entry.
Done. If I enter the same password, I get the same result
- make all hash the same length.
Not done. 'myPassword' hash is 8, 'MyVeryFavePassword' hash is 18.
- scramble the hash. So someone stealing the file can't figure out the password.
Not done.
2.
One way it is insecure is that someone systematically trying passwords of different lengths might gain wrongful access
3.
Replacing this password hashing with one built into your programming language or operating system or language would greatly improve security
"

"Authentication of you as a user
(are you who you say you are)

can be based on

1. **What you know**
2. **What you have**
3. **What you are**
4. **What you do**

"

"What you know
password
security question like ""what is the name of your grandmother?""

What you have
your phone
your card (credit card, student card, ...)
a cryptographic key on your device (private key shared with YouTube while signed in)

What you are
biometrics - things measured from your body
your fixed biometrics (fingerprint, face, iris ... for fingerprint scanner etc)

What you do
how you write your signature
how you speak a particular phrase
"

Authentication of you
as a user
(are you who you say you are)

can be based on

1. What you know
2. What you have
3. What you are
4. What you do

Weaknesses include that they may be

lost
stolen
spoofed
researched

Authentication of you as a user
(are you who you say you are)

based on

1. What you know
2. What you have
3. What you are
4. What you do

Each one may be insecure because it could be lost, stolen, spoofed, researched.

A common security measure to increase security because of this is

two-factor verification

Example:

Sign onto your banking app with your fingerprint.
Ask for a new withdrawal.
Bank asks you to enter the new code it is just sent by SMS to your phone.

"Passwords and other things are hashed so they can be rechecked each time they are used.

Two qualities a hashing

"Example:

If MySecretPassword produces the hash C152246C91EF62F553D2109B68698B19F7DD83328374ABC489920BF2E
using the SHA-256 algorithm the first time

MySecretPassword should produce

algorithm must:

Make same hash every time the same input is used.
Not decode in any way back to its original.

"

C152246C91EF62F553D2109B68698B19F7DD83328374ABC489920BF2E
every time MySecretPassword is hashed by the SHA-256 algorithm.

Actually, must be true for every hashing algorithm."

When you enter your password, it is most likely hashed by the hashing algorithm called

SHA-256

The SHA-256 hashing algorithm is used to protect

Unix passwords,
Bitcoin transactions,

unfinished

"A hash function that is used to check a file that has arrived
is exactly the same as
as the file that was sent is

a checksum
"

"Explanation:

A hash function is commonly used for passwords.
The hash is made by producing a one-way encription of the whole of the password.
Password entered next time → hash will match if the same.

A hash function is also commonly used for files.
The hash (checksum) is made by the sender producing a one-way encription of the whole of the file.
It travels with the file.
A hash (checksum) is made by the receiver producing a one-way encription of the whole of the file
File not exactly the same → checksum will not match.

More
Sender attaches checksum to file before sending - usually when saved, because it can take a long time.
Receiver produces their own checksum on the same file - are the

same.
Installation software often starts on the receiver's device by doing its own checksum check on the downloaded file.
Because it can take a fair amount of time for a large download, messages often displayed while this happens saying something like ""checking download"" Or ""integrity check""."

Asymmetric encryption
Data encrypted by the public key can only be decrypted by the private key of

the same user.

"Example:
I know Joan's public key.
I use Joan's public key to encrypt an email to her.
Only Joan's private key will be able to decript the message.
So, even if the email gets accidentally sent to a thousand users, only Joan will be able to decript it with her private key."

Asymmetric encryption
SPY wanted to send his secret information to BOSS.
What private or public keys will be needed for him to do this?

Only the public key of the BOSS.

"Explaination:

To encrypt a message to anyone so you know that they are the only one that can read it, all you need is their public key.

You don't need any keys yourself."

Asymmetric encryption
PREMIER wants EVERYONE to know this statement is genuinely from him, and no one else.

What keys does premier need to encrypt this statement?

Only the private key of PREMIER.

"Explaination:

To encrypt a message so everyone will know it is from you, all you need to do is to encrypt it with your own private key.

You don't need any more keys yourself."

Asymmetric encryption
Guarantee that only one particular person can decrypt your message – use **their public** key.
Show everyone that this message can only come from you – use **your own private** key.

Asymmetric encryption
Use software to generate both a public key and a private key for yourself.

In terms of your home, the **public** key is your street address which anyone who cares to know can find out;
The **private** key is the key to your front door which you keep very safe.

"Asymmetric encryption - quite slow - very secure.
Symmetric encryption - very fast - insecure at setup while getting the shared secret key to both parties.

Rivest, Shamir and Adelman (RSA) set up the first asymmetric encryption system.
RSA is still used extensively today.
Its main task is at the start of an exchange where it used to transmit

"One common RSA example
RSA is still used in a Virtual Private Network (VPN) to make connections between VPN service and VPN clients"

the secret shared keys so the faster symmetric encryption can take over for the bulk of the work.
"

Asymmetric encryption
The RSA algorithm generates its public key (made public) by multiplying two prime numbers (which are kept secret).
An encrypted message can be decrypted with these two prime numbers.
They are kept secret, you do know their product is the public key.
It is easy enough to write code that will step through the possibilities until the correct answer is found.
But this is not done because

for the code to work on the average computer when RSA uses two very large prime numbers, the time to find an answer is measured in lifetimes.

Imagine the public key is 91.
You could easily write code to go through the prime numbers, 2, 3, 5, 7, 11, ===

dividing 91 by each until the answer is another prime number.
You will find that one pair of prime numbers works (91 = 7 x 13)
You have cracked the code!
You can decrypt the message
