Bank of England Museum

THE FUTURE OF MONEY

The Future of Money

PACK 5

Data and Privacy

An education resource for students aged 11–14.

Contents

About the Future of Money exhibition

This resource collection is designed to accompany The Future of Money exhibition at the Bank of England Museum. The resources explore the links between the exhibition and a range of mathematical ideas, using exhibition objects and themes as a starting point for discussion and mathematical problem-solving. These activities will work in the classroom or at home and are designed for students aged 11-14.

The resources contain supporting notes for teachers, images from the exhibition and student activity sheets. There are five resource packs, each focusing on a different exhibition theme:

Pack 1: What is Money?

Topics covered include: compound measures; units of measurement; problem solving; probability

Pack 2: Futureproofing Today's Systems

Topics include: data collection and questionnaires; analysing data; bar charts; pie charts.

Pack 3: Future Methods of Payment

Topics include: prime numbers and their properties; divisibility rules; sampling methods; calculating percentages

Pack 4: Education, Environment, Sustainability

Topics include: 3D shapes; adding, subtracting and dividing with decimals; problem solving

Pack 5: Data and Privacy

Topics include: sequences and patterns; problem solving; inverse operations; division with remainders

Whichever activities your students complete, we'd love to see the results, so please share them with @boemuseum **#TheFutureofMoney**

Idea in focus: Data security

Mathematics curriculum topics: Sequences and patterns; problem solving; inverse operations; division with remainders

When we hand over coins and banknotes we want to make sure that we're handing them to the right people, and that we're going to get what we're expecting in return. We have the same expectations for digital payments, but as well as exchanging money, digital payments involve sharing other forms of data.

Apps, websites and other digital providers that we interact with collect data for various reasons. Some data is used to verify our identity; and some is intended to target advertising based on things we have bought previously. Sometimes, if we agree, this information is sold to third parties who might also want to sell us products.

In the UK there are strict guidelines on how personal and financial data can be collected and used, with heavy penalties for misuse. Organisations have a duty to protect the data they collect, and this is partly achieved through encryption, which is underpinned by a number of mathematical principles.

Student activity 1: (Un)scramble

Task

Below are some sayings about money that have been scrambled (along with the person or culture that they are thought to have come from).

Your first challenge is to unscramble the sayings.

Your second challenge is even more important: Can you explain what process was used to scramble each one, and how to undo it? Every phrase is scrambled in a different way.

1. brevorp itnahsa - hcir emoceb dna tsaef tonnac eno
2. hcterts ruoy mra on rehtruf naht ruoy eveels lliw hcaer - hsikrut brevorp
3. Money isonl yatoo lItwi lltak eyouw herev eryou wishb utitw illno trepl aceyo uasth edriv erAyn Randx
4. yenoM netfo stsoc umoot laRhc laWhp emEod xnosr
5. Uif cftu uijoht jo mjgf bsf gsff. Tpoh ujumf cz Cveez ef Tzmwb boe Mfx Cspxo

None of the sentences above are scrambled randomly because that would be useless as a form of encryption - even the people you wanted to read a message wouldn’t be able to undo a random scramble. Each message is scrambled using a pattern - a slightly more complicated one each time.

Mathematics is sometimes described as the study of patterns and so is an incredibly important part of the science of encryption.

Student activity 1: Answers and supporting notes for teachers

Task

1. One cannot feast and become rich - Ashanti proverb
    - The entire sentence is written backwards

2. Stretch your arm no further than your sleeve will reach - Turkish proverb
    - Each word is written backwards

3. Money is only a tool. It will take you wherever you wish, but it will not replace you as the driver - Ayn Rand
    - The spaces have been removed from the sentence, and then the letters have been split into groups of 5

4. Money often costs too much. - Ralph Waldo Emerson
    - The same process was used to encrypt this as for #4, except each group of 5 letters was reversed

5. The best things in life are free. Song title by Buddy de Sylva and Lew Brown
    - Each letter was replaced with the next letter in the alphabet (i.e. a was replaced with b, b was replaced with c)

Student activity 2: Caesar cipher

Encryption has played important roles throughout history, allowing the military to keep secrets from their enemies and inventors to keep designs secret from their competitors.

A cipher is an algorithm for performing encryption and decryption: a clear set of instructions that can be followed to hide the meaning of a word or phrase. One of the most famous examples of an encryption algorithm is the Caesar cipher, which was named after the Roman general, Julius Caesar. The algorithm works like this:

Swap each letter in the plaintext for the one k *places to the* ***right*** *in the alphabet.*

"Plaintext" is the word for the unencrypted message and *k* is a number between 1 and 25 chosen by the person who is encrypting the message. K stands for "key", and the key is what we use to 'lock' (encrypt) and 'unlock' (decrypt) the message.

The Caesar cipher can be represented mathematically by using numbers to replace each letter of the alphabet:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

First, we choose a "key", *k*, which is a number between 1 and 25.

We can then encrypt messages using the following algorithm:

Step 1: Swap the letter for the number shown in the table.
Step 2: Add *k* to that number (where *k* is a number between 1 and 25)
Step 3: Swap the new number for the letter shown in the table.

If the number goes past 25, we need to go back to 0 and carry on from there.

Task

1. Encrypt the following phrases using the given values for *k*:
    a. *k* = *5*: Can you keep a secret?
    b. *k* = *3*: The meeting is at five

2. These messages have been encrypted using the given values for *k*. Can you decrypt them?
    a. *k* = *2*: Rfc Dsrspc md Kmlcw
    b. *k* = *7*: Dxxi rhnk ixklhgte wtmt ltyx

Student activity 2: Answers and supporting notes for teachers

Task

1.
    a. hfs dtz pjju f xjhwjy
    b. Wkh phhwlqj lv dw ilyh

2. Some students may need a hint: If you add to encrypt the messages, what must you do to decrypt them?
    a. The Future of Money
    b. Keep your personal data safe

Student activity 3: Affine ciphers

Throughout history secret battles have been fought between those who want to hide information and those who want to uncover it, forcing ciphers to become more complicated and imaginative over time. Using numbers to represent letters makes it easier to implement more complicated ciphers. One example is the affine cipher, which is used to rearrange the alphabet in a slightly more complicated way than a Caesar cipher, with a pattern that is much less easy to spot.

Work through the following task to understand how the affine cipher works:

In the table below, each letter is represented by a number in the cell below it.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Multiply each number by 3, and then add 2:																									
2		8				20				32								56					71		
		8				20												4					19		
C	F	I																					T		

Task

1. The third row of the table describes a calculation: perform this calculation on each number in the second row and write the result in the corresponding cell of the fourth row. Some have been completed for you.

2. Divide each number in the fourth row by 26 and **write the remainder** in the fifth row. Some have been completed for you.

3. When you've completed the fifth row you can use these numbers to write in the re-ordered alphabet in the bottom row. (0 is A, 1 is B, 2 is C and so on)

You can then use this table to encrypt and decrypt messages: find the first letter of your message in the top row and swap it for the letter in the same column of the bottom row.

Student activity 3: Answers and supporting notes for teachers

It might be helpful to complete activity 2 (Caesar cipher) ahead of activity 3, but it is not essential.

The completed table should look like this.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Multiply each number by 3, and then add 2:																									
2	5	8	11	14	17	20	23	26 0	29 3	32 6	35 9	38 12	41 15	44 18	47 21	50 24	53 1	56 4	59 7	62 10	65 13	68 16	71 19	74 22	77 25
C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

Messages can be encrypted by swapping each letter in the top row for the corresponding letter in the bottom row. For example, BANK encrypts to FCPK.

To decrypt a message, find each letter in the bottom row and swap it for the corresponding letter in the top row (so FCPK decrypts back to BANK).

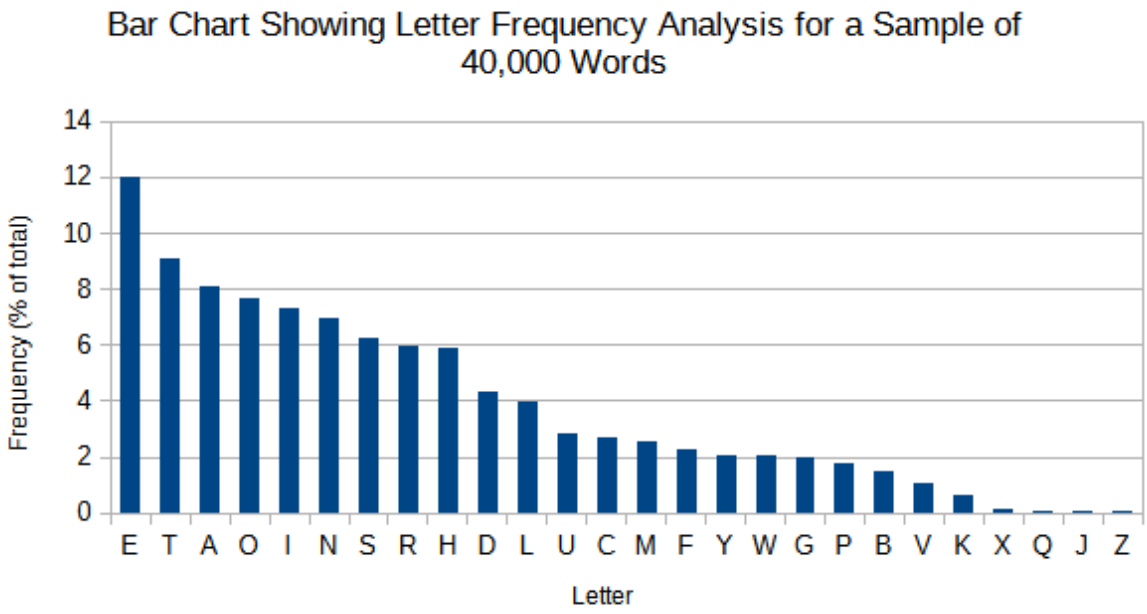
Extend this:

Other rearrangements of the alphabet can be rearranged by changing the numbers used in the central row (such as “Multiply each number by 5, and then add 4”). The second number can be anything from 1 – 25, but the first number can only be certain values.

An interesting challenge for some students is to experiment with different values for the multiplier, discover which work and which don’t work, and to try to explain why (only the multipliers 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 will result in a rearranged alphabet that doesn’t miss out or duplicate any letters).

Student activity 4: Letter frequency analysis

The bar chart below shows the relative frequencies of letters in a sample of 40,000 English words.



Data source: **https://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html**

Task

The following text was written in English and then every letter was swapped for a different letter. Can you use the information above to work out what it says?

Hint: Count how many times each letter occurs and compare this with the chart above.

ZRWU SAXCNPCIGWVM ZCSRVWKEC SIV AVLY OAPG OWZR XIZI ZRIZ RIU NCCV CVSPYFZCX OWZR I QAVAILFRINCZWS SWFRCP, NEZ WZ WU I MAAX WLLEUZPIZWAV ZRIZ SWFRCPU IPCV'Z ILL WVJWVSWNLC! ZRC QIZRCQIZWSU NCRWVX QAXCPV SWFRCPU UESR IU ZRAUC ZRIZ NIVGU EUC ZA GCCF ZRC WVHAPQIZWAV ZRCY RALX INAEZ YAE UIHC, AP ZRIZ CVINLC SPYFZASEPPCVSWCU ZA NC UCSEPC IU OCLL IU IVAVYQAEU QIGCU ZRC WVHAPQIZWAV ZRCY RWXC SAVUWXCPINLY RIPXCP ZA EVSAJCP. WV HISZ, ZRC OCIGCUZ FIPZ AH QAXCPV CVSPYFZWAV WU EUEILLY VAZRWVM IZ ILL ZA XA OWZR ZRC SRAWSC AH SWFRCP: ZRC OCIGCUZ FIPZ WU VCIPLY ILOIYU ZRC CVX EUCP! WH IVYNAXY SIV MECUU YAEP FIUUOAPX WZ XACUV'Z QIZZCP RAO UCSEPCLY CVSPYFZCX ZRC WVHAPQIZWAV NCRWVX WZ WU!

Student activity 4: Answers and supporting notes for teachers

The text, when decrypted, reads:

> “This codebreaking technique can only work with data that has been encrypted with a monoalphabetic cipher, but it is a good illustration that ciphers aren’t all invincible! The mathematics behind modern ciphers such as those that banks use to keep the information they hold about you safe, or that enable cryptocurrencies to be secure as well as anonymous makes the information they hide considerably harder to uncover. In fact, the weakest part of modern encryption is usually nothing at all to do with the choice of cipher: the weakest part is nearly always the end user! If anybody can guess your password it doesn’t matter how securely encrypted the information behind it is!”

A successful letter frequency analysis of this text matches the bar chart down to the seventh most common letter.

Object in focus: Nando's loyalty card

Mathematics curriculum topics: Lowest common multiple; multiples

Loyalty cards are offered by all sorts of retailers, from restaurant chains to supermarkets. They offer us benefits like in-store credits and members-only discounts, but what do they get in return?

To a degree, loyalty cards encourage customers to keep using the same retailer rather than changing to a competitor. To use a retailer's loyalty card a customer must agree that the retailer can collect data about their shopping habits. This can be used to target advertising to that customer more accurately, and means the retailer gains a better understanding of the habits of different demographic groups e.g. young people aged 18-24.

Student activity 5: Spicy sauce

A supermarket recorded how often 3 customers bought a bottle of spicy sauce from a popular brand in the last year:

Customer A bought a bottle every 3 days.

Customer B bought a bottle every 5 days.

Customer C bought a bottle every 6 days.

The supermarket is releasing its own brand of spicy sauce and wants to do it on a day when the largest number of people are predicted to buy spicy sauce.

If customers A, B and C all bought spicy sauce on 29th January, what is the best date for the supermarket to release their sauce?

Student activity 5: Answers and supporting notes for teachers

If customer A bought a bottle on day 0, then they are likely to buy more bottles on days 3, 6, 9, 12, …

If customer B bought a bottle on day 0, then they are likely to buy more bottles on days 5, 10, 15, 20, …

If customer C bought a bottle on day 0, then they are likely to buy more bottles on days 6, 12, 18, 24, …

We are looking to see which day number is in the 3-, 5- and 6-times table (which is the "lowest common multiple" of 3, 5 & 6).

Solution 1:

Write out the 3, 5 and 6 times tables until we reach the smallest number that is in all three:

3, 6, 9, 12, 15, 18, 21, 24, 27, **30**

5, 10, 15, 20, 25, **30**

6, 12, 18, 24, **30**

The next day when all three customers should buy bottles is 30 days after 29th January, which is 28th February.

Solution 2:

Using prime factors:

Prime factorisation of 3 = 3

Prime factorisation of 5 = 5

Prime factorisation of 6 = 2 × 3

The lowest common multiple is obtained by multiplying together one of each prime number that is represented in any of the prime factorisations: 2 × 3 × 5 = **30**.

The next day when all three customers should buy bottles is 30 days after 29th January, which is 28th February.