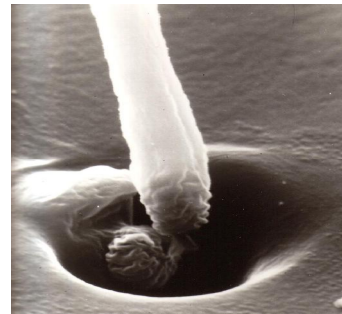


How do sharks and crabs sense depth? Crabs in space and out of their depth

The Crabs in Space team used a very simple mathematical calculation to prove a fundamental part of their research. Applying a branch of mathematics known as **hydrostatics** enabled them to understand how a change in water pressure can stimulate the crab's balancing system. Hydrostatics describes and predicts what happens to fluids (this includes gases and liquids) at rest – **hydrodynamics** is the equivalent study for fluids in motion.

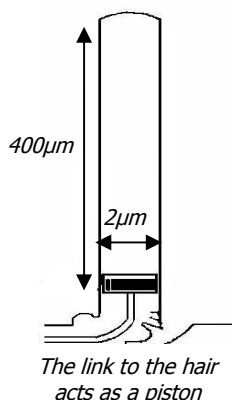
The crab's balancing system is made up of a liquid-filled 'vestibular' cavity with sensory hairs inside. These tiny thread hairs are linked to mechanoreceptors, telling the crab that it needs to re-balance. The team had discovered that a movement of just 17 nanometres (17 billionths of a metre) was enough to stimulate the hair mechanoreceptor.

But nobody had yet understood how this system could work under water, since most similar work had been done on animals with gas-filled organs linked to their vestibular systems.



The crab's thin sensory hair is linked to a mechanoreceptor

Hydrostatics shows that gases compress considerably under pressure, but liquids only compress by tiny amounts – for example, seawater has a **compressibility** of 44×10^{-6} per bar (a bar is a unit of pressure which is approximately equal to atmospheric air pressure at sea level). This means that for each increase in pressure by 1 bar, the volume of the water reduces by 44 millionths.



The link to the hair acts as a piston

The team realised that as a crab travelled into deeper water and the water pressure increased, the minute change in the volume of the liquid in the hair was enough to move the link to the mechanoreceptor. The link to the hair worked as a piston - as the volume of the liquid inside the hair reduced under increasing pressure, it disturbed the mechanoreceptor and sent a sensory signal to the crab's brain.

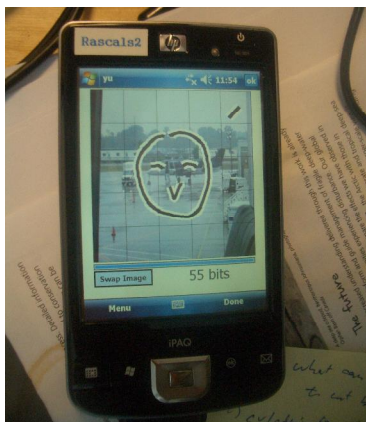
They considered the hair as a cylinder filled with water-like liquid but with incompressible walls. The hair is 2 micrometres (2 millionths of a metre or $2 \mu\text{m}$) in diameter and $400 \mu\text{m}$ long. The volume of the liquid is given by $\pi \times (\text{radius})^2 \times \text{length}$.

If the crab is exposed to an extra 1 bar of pressure, the volume of the liquid reduces. Because the walls of the hair are incompressible, the diameter of the liquid remains constant - so only the length of the liquid cylinder changes. So, using the compressibility of seawater given above, the length of the cylinder of liquid reduces by $44 \times 10^{-6} \times 400 = 17600 \times 10^{-6} \mu\text{m}$ (or 17.6 nanometres) – exactly the displacement needed to stimulate the mechanoreceptor of the crab's balancing system.

Graphical Passwords: will your doodle keep the hackers away?

Computer security experts often tell us not to choose an easy to guess word as a password – for example, the user’s name or date of birth.

The Graphical Passwords team have been working on a new password system that is more secure. Their tests suggest that the Background Draw A Secret (BDAS) graphical passwords are up to 40 per cent stronger (and yet easier for the user to remember) than a typical eight character password made up of letters, numbers and symbols.



Just a simple smiley face password, as above, can have a strength of 55 bits

For example, traditional passwords such as **C4hjy!89** would have a strength of about 53 bits. The very simple smiley face above would have a similar strength. But a slightly more complex picture would be much stronger.

So how do computer scientists work out how ‘strong’ passwords can be?

In 1948, in a world where secure communication and code-breaking were vitally important, an American electrical engineer and mathematician called Claude Shannon published a ground-breaking book. “**The Mathematical theory of Communication**” established a new branch of applied mathematics now known as **information theory** which enabled mathematicians to quantify information. In particular, he came up with a way of measuring how much information there is in a message, called **information entropy**.

Entropy is often discussed in physics and chemistry and is a gauge of the disorder or chaos in a system. Similarly, **information entropy** can measure how much redundancy there is in a message, or, conversely, how much information it carries. A high entropy means there is a lot of uncertainty, so the message carries a lot of new information. So the higher the entropy, the more difficult a password is to guess.

For example, a message telling you: "You are at the 2008 Royal Society Summer Exhibition" doesn't tell you anything you don't know – you knew that would happen when you set out this morning. But telling you: "You are at the Graphical Passwords stand" does give you new information.

The overall entropy of an event X is calculated as the sum of each possible outcome x within X . Let's write the probability of a particular outcome as $p(x)$. So if $p(x) = 1$, then we know that that particular outcome will definitely happen – in information terms, this means a content of 0.

Putting in some other conditions, it turns out that taking the logarithm - ie $\log(p(x))$ - is the best way to handle this measure of information. Logarithms can be calculated in any base, but if the chosen base is 2 then we say that the information is in **bits**, ideal for when you are talking about computer information.

So the **information entropy** is computed mathematically as:

$$H(X) = - \sum_{\text{all possible } x} p(x) \log_2 p(x)$$

Now consider another situation where two events are equally likely to happen, such as tossing a fair coin. So if we consider tossing a coin, the entropy is

$$-(\frac{1}{2} \log_2(1/2) + \frac{1}{2} \log_2(1/2)) = \mathbf{1 \text{ bit}}$$

In general, the more equally likely events n there are, $\log(n)$ increases and the entropy goes up as the amount of information you get is greater.

Suppose you are choosing an eight letter password from the 26 lower case letters. The **theoretical entropy** is

$$8 \times \log_2 26 \approx 8 \times 4.7 \approx \mathbf{37.6 \text{ bits}}$$

But choosing the password from digits and upper and lower case letters and other symbols, gives 95 characters to choose from. So the entropy is

$$8 \times \log_2 95 \approx 8 \times 6.6 \approx \mathbf{53 \text{ bits}}$$

However, the **practical strength** of commonly used 8-character passwords is far less than 53 bits since people often choose memorable words and names. A modern desktop computer can search through about 2^{40} (around 1,000 billion) passwords in 24 hours, and the speed of computers is fast increasing. So passwords with a bit-strength of less than 40 bits can be easily guessed, when hackers are able to make repeated tries to verify their guess.

In the BDAS system, it isn't just different characters that make up passwords and affect their strength. BDAS password strength comprises:

- **number** of strokes (a stroke is complete when the pen is lifted up)
- **length** or number of grid cells a drawing cuts through
- **size** of the grid and the grid size
- **order** of strokes.

The team calculated the total number of passwords of a length smaller than 13 on a 5x5 grid is more than 2^{53} - the total number of 8-character text passwords! The smiley face overleaf has a stroke count of 5 and a password length of 17 - the total number of passwords of such or less complexity in BDAS is around 2^{55} for a 5x5 grid.

The team found that the average strength of the BDAS passwords created by participants in their experiments could be as high as 60-70 bits, and 95% users were able to recreate their passwords within three attempts one week later.

Wonder in carbon land: how do you hold a molecule?

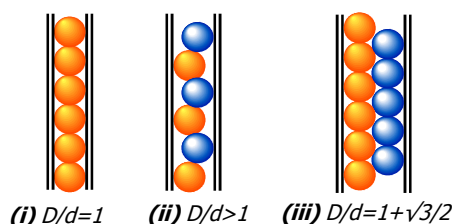
The Carbon Land team discovered that when their fullerenes were packed into nanotubes, the formations they packed themselves into depended on the diameter of the nanotube. In particular, they noticed some regular formations – linear one-dimensional chains, zigzags, double helices and two molecule layers.

In fact, the team's laboratory experiments enabled them to see nature displaying an area of mathematics that has fascinated mathematicians for centuries – how to **pack spheres**.

As spheres do not fit neatly together like cubes, mathematicians want to find out the most efficient way of packing them with the least empty space between. The problem has exercised the minds of some of the greatest mathematicians over the past four centuries, including **Johannes Kepler**, **Isaac Newton** and **Carl Friedrich Gauss**.

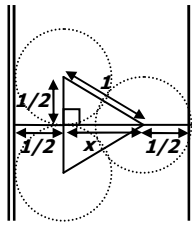
But the chemists' work shows that the problem is not only an interesting puzzle to challenge brilliant minds - its practical applications are clear.

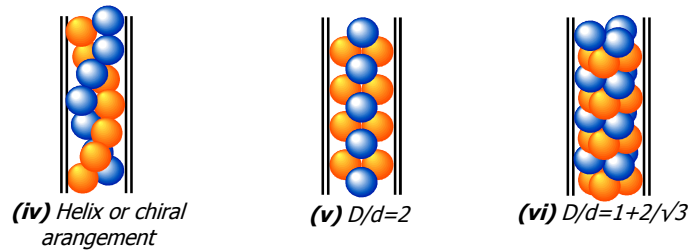
They are looking at a particular case where the balls (fullerenes which are of fixed size) are packed into a tube (carbon nanotubes in a range of different sizes). Suppose the diameter of the nanotube is D and the diameter of the fullerene is d . The arrangement of the balls in the tube depends on the ratio of the tube diameter to the ball diameter.



So when the balls only just fit in the tube (ie $D = d$ and $D/d = 1$), they form a single column (see (i)). But if D is slightly greater than d (so $D/d > 1$), the balls use the extra space to fall into a zig-zag pattern across the tube (ii).

This is fine until D/d reaches the critical value of $1+\sqrt{3}/2$ (about 1.866). At this point, each orange ball touches the orange ball below and each blue ball touches the blue ball below (iii). In fact, each ball is touching four others and any three successive balls form an equilateral triangle across the tube.

EXPLAINER	
	<p>Supposing the spheres are of diameter 1, the diameter of the nanotube is $1+x$.</p> <p>Using Pythagoras: $1^2 = (1/2)^2 + x^2$ $x^2 = 1 - 1/4 = 3/4$ So $x = \sqrt{3}/2$ and the diameter of the nanotube is $1 + \sqrt{3}/2$</p>



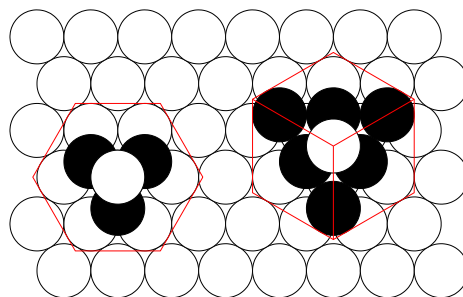
If D/d gets greater still, these triangles can tilt over either way, but for efficient packing, all must tilt in the same direction. This creates a **helix** or spiral effect, either right-handed or left (**iv**). This 'broken symmetry' is known as a **chiral** effect and occurs when a symmetric or flat arrangement of balls in the cross section of the tube becomes tilted.

When D/d reaches 2, the cross section of the tube would consist of pairs of balls sitting at right angles to the pairs both above and below (**v**).

The next critical point is when D/d reaches $1 + 2/\sqrt{3}$ (about 2.155) when three balls will just fit in the cross section of the tube (**vi**). This value can be found by a similar method to case (iii), using simple geometry and Pythagoras' theorem.

If we could let the diameter of the cylindrical nanotube become infinitely large, the balls would pack themselves in one of the two most efficient packing arrangements – **face centred cubic** or **hexagonal close packed**.

Both these packing arrangements involve layers of spheres which sit in triangles in the plane of the layer. The layers then sit atop one another, in the hollows. In **hexagonal close packing** the third layer is directly over the first – imagine filling a snooker triangle with balls and then building layers on top to form a pyramid. In **face centred cubic packing** the spheres form a cube shape, with each layer shifted until eventually the fourth layer sits over the first - imagine a cube with a sphere at each corner and in the centre of each face



Hexagonal close packing and face centred cubic packing

The **Kissing Number** is the maximum number of spheres of radius one which can touch a single given sphere also of radius one. In three dimensions, Isaac Newton (1642 - 1727) correctly conjectured this number was 12 (six in the same plane, three in the plane above and three in the plane below) but a proof wasn't offered until 1874 and several more concise proofs were discovered as late as the 1950's.

In 1611, Kepler conjectured that these two 'close packings' were the most efficient way of packing spheres. However, what became known as **Kepler's Problem** did not have a satisfactory proof until 1998, when Thomas Hales at the University of Pittsburgh announced that he had checked every possibility.

Although most of the problems have now been solved for packing in three dimensional space, today's mathematicians are still working on the solutions for four, five and every higher dimensional space!