

# Session 15 – Breaking the Vigenère cipher

## European section – Season 3

# How to do it ?

# How to do it ?

- 1 Find the probable length of the key,  $n$ .

# How to do it ?

- 1 Find the probable length of the key,  $n$ .
- 2 Divide the cipher text into  $n$  groups of letters.

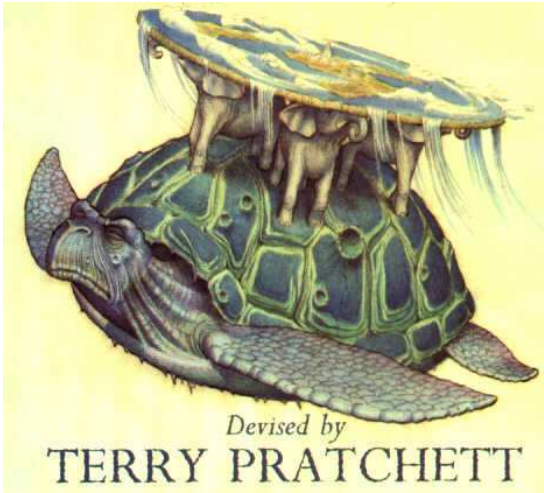
# How to do it ?

- 1 Find the probable length of the key,  $n$ .
- 2 Divide the cipher text into  $n$  groups of letters.
- 3 Apply frequency analysis to each group, to find each Caesar shift.

Use a software to break a  
Vigenère cipher.

# About the plain texts

# About the plain texts



## About the plain texts



## Cipher 1 – Keyword : LUCKY

They say that the prospect of being hanged in the morning concentrates a man's mind wonderfully; unfortunately, what the mind inevitably concentrates on is that, in the morning, it will be in a body that is going to be hanged. The man going to be hanged had been named Moist von Lipwig by dotting if unwise parents, but he was not going to embarrass the name, insofar as that was still possible, by being hung under it. To the world in general, and particularly on that bit of it known as the death warrant, he was Alfred Spangler.

## Cipher 1 – Keyword : LUCKY

And he took a more positive approach to the situation and had concentrated his mind on the prospect of not being hanged in the morning, and, most particularly, on the prospect of removing all the crumbling mortar from around a stone in his cell wall with a spoon. So far the work had taken him five weeks and reduced the spoon to something like a nail file. Fortunately, no one ever came to change the bedding here, or else they would have discovered the world's heaviest mattress.

It was a large and heavy stone that was currently the object of his attentions, and, at some point, a huge staple had been hammered into it as an anchor for manacles. Moist sat down facing the wall, gripped the iron ring in both hands, braced his legs against the stones on either side, and heaved.

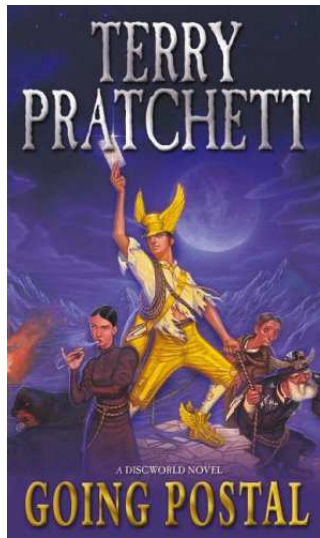
His shoulders caught fire, and a red mist filled his vision, but the block slid out with a faint and inappropriate tinkling noise. Moist managed to ease it away from the hole and peered inside.

At the far end was another block, and the mortar around it looked suspiciously strong and fresh.

Just in front of it was a new spoon. It was shiny.

As he studied it, he heard the clapping behind him. He turned his head, tendons twanging a little riff of agony, and saw several of the wardens watching him through the bars.

# Cipher 1 – Keyword : LUCKY



Some of the things you could learn up a drainpipe at night were surprising. For example, people paid attention to small sounds—the click of a window catch, the clink of a lock pick—more than they did to big sounds, like a brick falling into the street or even (for this was, after all, Ankh-Morpork) a scream.

These were loud sounds, which were, therefore, public sounds, which, in turn, meant they were everyone's problem and, therefore, not mine. But small sounds were nearby and suggested such things as stealth betrayed, and were, therefore, pressing and personal.

## Cipher 2 – Keyword : PARANO

Therefore, he tried not to make little noises.  
Below him, the coach yard of the Central Post Office buzzed like an overturned hive. They'd got the turntable working really well now. The overnight coaches were arriving and the new Überwald Flyer was gleaming in the lamplight. Everything was going right, which was, to the nighttime climber, why everything was going wrong.

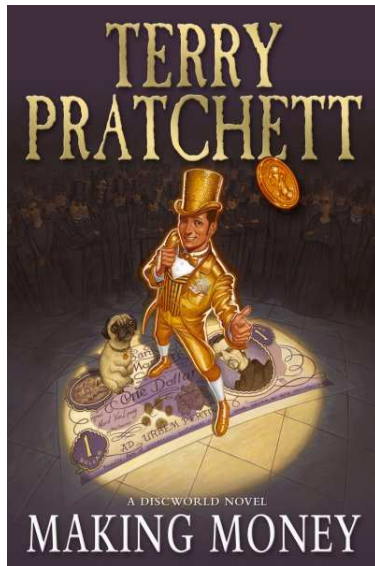
## Cipher 2 – Keyword : PARANO

The climber thrust a brick key into soft mortar, shifted his weight, moved his foot—

Damn pigeon! It flew up in panic, his other foot slipped, his fingers lost their grip on the drainpipe, and when the world had stopped churning, he was owing the postponement of his meeting with the distant cobbles to his hold on a brick key, which was, let's face it, nothing more than a long, flat nail with a T-piece grip.

And you can't bluff a wall, he thought. If you swing, you might get your hand and foot on the pipe, or the key might come out.

## Cipher 2 – Keyword : PARANO



## Cipher 3 – Keyword : AIRBAG

Sam Vimes sighed when he heard the scream, but he finished shaving before he did anything about it.

Then he put his jacket on and strolled out into the wonderful late spring morning. Birds sang in the trees, bees buzzed in the blossom. The sky was hazy though, and thunderheads on the horizon threatened rain later. But for now, the air was hot and heavy. And in the old cesspit behind the gardener's shed, a young man was treading water.

Well ... treading, anyway.

Vimes stood back a little way and lit a cigar. It probably wouldn't be a good idea to employ a naked flame any nearer to the pit. The fall from the shed roof had broken the crust.

“Good morning!” he said cheerfully.

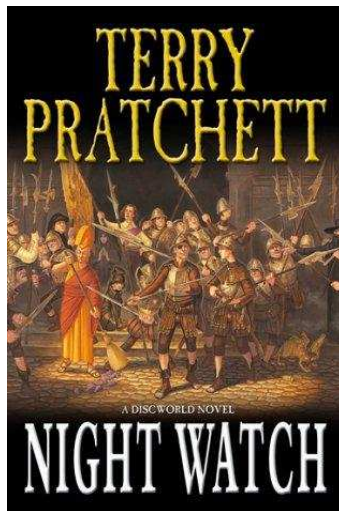
“Good morning, Your Grace,” said the industrious treadler. The voice was higher pitched than Vimes expected and he realized that, most unusually, the young man in the pit was in fact a young woman. It wasn’t entirely unexpected – the Assassins’ Guild was aware that women were at least equal to their brothers when it came to inventive killing – but it nevertheless changed the situation somewhat.

## Cipher 3 – Keyword : AIRBAG

"I don't believe we've met?" said Vimes. "Although I see you know who I am. You are ... ?"

"Wiggs, sir," said the swimmer. "Jocasta Wiggs. Honored to meet you, Your Grace."

"Wiggs, eh?" said Vimes. "Famous family in the Guild. 'Sir' will do, by the way. I think I once broke your father's leg?"



Everything starts somewhere, although many physicists disagree.

But people have always been dimly aware of the problem with the start of things. They wonder aloud how the snowplow driver gets to work, or how the makers of dictionaries look up the spelling of the words. Yet there is the constant desire to find some point in the twisting, knotting, raveling nets of space-time on which a metaphorical finger can be put to indicate that here, here, is the point where it all began. . .

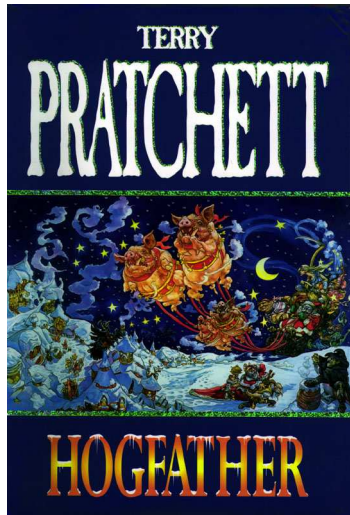
Something began when the Guild of Assassins enrolled Mister Teatime, who saw things differently from other people, and one of the ways that he saw things differently from other people was in seeing other people as things (later, Lord Downey of the Guild said, "We took pity on him because he'd lost both parents at an early age. I think that, on reflection, we should have wondered a bit more about that").

But it was much earlier even than that when most people forgot that the very oldest stories are, sooner or later, about blood.

Later on they took the blood out to make the stories more acceptable to children, or at least to the people who had to read them to children rather than the children themselves (who, on the whole, are quite keen on blood provided it's being shed by the deserving), and then wondered where the stories went.

And earlier still when something in the darkness of the deepest caves and gloomiest forests thought: what are they, these creatures? I will observe them. . .

# Cipher 4 – Keyword : MUSIC



## Cipher 5 – Keyword : FITTER

Against the stars a turtle passes, carrying four elephants on its shell.

Both turtle and elephants are bigger than people might expect, but out between the stars the difference between huge and tiny is, comparatively speaking, very small.

But this turtle and these elephants are, by turtle and elephant standards, big. They carry the Discworld, with its vast lands, cloudscapes, and oceans.

People don't live on the Disc any more than, in less hand-crafted parts of the multiverse, they live on balls.

Oh, planets may be the place where their body eats its tea, but they live elsewhere, in worlds of their own which orbit very handily around the center of their heads.

When gods get together they tell the story of one particular planet whose inhabitants watched, with mild interest, huge continent-wrecking slabs of ice slap into another world which was in astronomical terms, right next door—and then did nothing about it because that sort of thing only happens in Outer Space. An intelligent species would at least have found someone to complain to. Anyway, no one seriously believes in that story, because a race quite that stupid would never even have discovered slood.

People believe in all sorts of other things, though. For example, there are some people who have a legend that the whole universe is carried in a leather bag by an old man.

## Cipher 5 – Keyword : FITTER

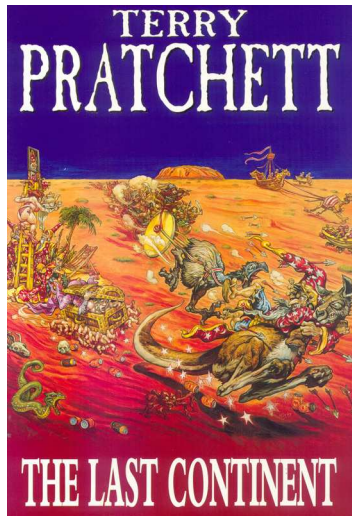
They're right, too.

Other people say: hold on, if he's carrying the entire universe in a sack, right, that means he's carrying himself and the sack inside the sack, because the universe contains everything. Including him. And the sack, of course. Which contains him and the sack already. As it were.

To which the reply is: well?

All tribal myths are true, for a given value of "true."

# Cipher 5 – Keyword : FITTER



It was a moonless night, which was good for the purposes of Solid Jackson.

He fished for Curious Squid, so called because, as well as being squid, they were curious. That is to say, their curiosity was the curious thing about them.

Shortly after they got curious about the, lantern that Solid had hung over the stern of his boat, they started to become curious about the way in which various of their number suddenly van-ished skyward with a splash.

Some of them even became curious—very briefly curious—about the sharp barbed thing that was coming very quickly toward them.

## Cipher 6 – Keyword : HAPPY

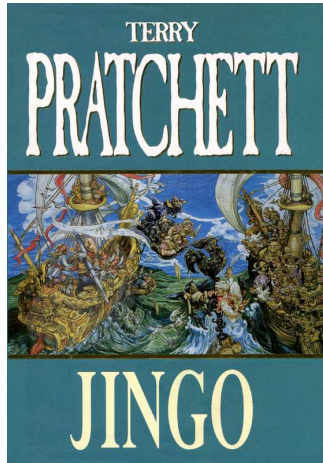
The Curious Squid were extremely curious. Unfortunately, they weren't very good at making connections.

It was a very long way to this fishing ground, but for Solid the trip was usually well worth it. The Curious Squid were very small, harmless, difficult to find and reckoned by connoisseurs to have the foulest taste of any creature in the world. This made them very much in demand in a certain kind of restaurant where highly skilled chefs made, with great care, dishes containing no trace of the squid whatsoever.

Solid Jackson's problem was that tonight, a moonless night in the spawning season, when the squid were especially curious about everything, the chef seemed to have been at work on the sea itself.

There was not a single interested eyeball to be seen. There weren't any other fish either, and usually there were a few attracted to the light. He'd caught sight of one. It had been making through the water extremely fast in a straight line.

# Cipher 6 – Keyword : HAPPY



## Cipher 7 – Keyword : WALLS

There is where the gods play games with the lives of men, on a board which is at one and the same time a simple playing area and the whole world.

And Fate always wins.

Fate always wins. Most of the gods throw dice but Fate plays chess, and you don't find out until too late that he's been using two queens all along.

Fate wins. At least, so it is claimed. Whatever happens, they say afterwards, it must have been Fate.

Gods can take any form, but the one aspect of themselves they cannot change is their eyes, which show their nature. The eyes of Fate are hardly eyes at all – just dark holes into an infinity speckled with what may be stars or, there again, may be other things.

## Cipher 7 – Keyword : WALLS

He blinked them, smiled at his fellow players in the smug way winners do just before they become winners, and said:

"I accuse the High Priest of the Green Robe in the library with the double-handed axe."

And he won.

He beamed at them.

"No one likeh a poor winner," grumbled Offler the Crocodile God, through his fangs.

"It seems that I am favoring myself today," said Fate.

"Anyone fancy something else?"

The gods shrugged.

## Cipher 7 – Keyword : WALLS

"Mad Kings?" said Fate pleasantly. "Star-Crossed Lovers?"

"I think we've lost the rules for that one," said Blind Io, chief of the gods.

"Or Tempest-Wrecked Mariners?"

"You always win," said Io.

"Floods and Droughts?" said Fate. "That's an easy one." A shadow fell across the gaming table. The gods looked up.

"Ah," said Fate.

"Let a game begin," said the Lady.

# Cipher 7 – Keyword : WALLS

TERRY  
PRATCHETT



INTERESTING  
TIMES

A DISCWORLD NOVEL

## Cipher 8 – Keyword : ALIEN

Now consider the tortoise and the eagle.

The tortoise is a ground-living creature. It is impossible to live nearer the ground without being under it. Its horizons are a few inches away. It has about as good a turn of speed as you need to hunt down a lettuce. It has survived while the rest of evolution flowed past it by being, on the whole, no threat to anyone and too much trouble to eat. And then there is the eagle. A creature of the air and high places, whose horizons go all the way to the edge of the world. Eyesight keen enough to spot the rustle of some small and squeaky creature half a mile away. All power, all control. Lightning death on wings. Talons and claws enough to make a meal of anything smaller than it is and at least take a hurried snack out of anything bigger.

## Cipher 8 – Keyword : ALIEN

And yet the eagle will sit for hours on the crag and survey the kingdoms of the world until it spots a distant movement and then it will focus, focus, focus on the small shell wobbling among the bushes down there on the desert. And it will leap . . .

And a minute later the tortoise finds the world dropping away from it. And it sees the world for the first time, no longer one inch from the ground but five hundred feet above it, and it thinks: what a great friend I have in the eagle.

## Cipher 8 – Keyword : ALIEN

And then the eagle lets go.

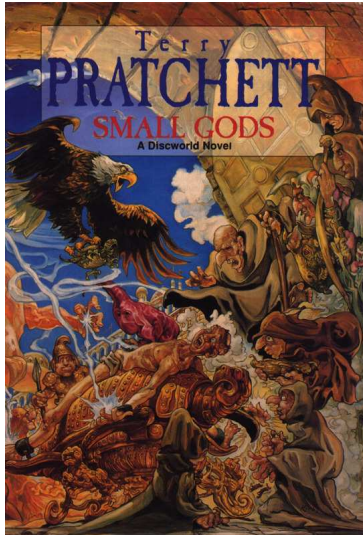
And almost always the tortoise plunges to its death.

Everyone knows why the tortoise does this. Gravity is a habit that is hard to shake off. No one knows why the eagle does this. There's good eating on a tortoise but, considering the effort involved, there's much better eating on practically anything else. It's simply the delight of eagles to torment tortoises.

But of course, what the eagle does not realize is that it is participating in a very crude form of natural selection.

One day a tortoise will learn how to fly.

# Cipher 8 – Keyword : ALIEN



If Youth, throughout all history, had had a champion to stand up for it; to show a doubting world that a child can think; and, possibly, do it practically, you wouldn't constantly run across folks today who claim that "a child don't know anything." A child's brain starts functioning at birth; and has, amongst its many infant convolutions, thousands of dormant atoms, into which God has put a mystic possibility for noticing an adult's act, and figuring out its purport.

Up to about its primary school days a child thinks, naturally, only of play. But many a form of play contains disciplinary factor. "You can't do this," or "that puts out out," shows a child that it must think, practically, or fail. Now, if, throughout childhood, a brain has no opposition, it is plain that it will attain a position of "status quo," as with our ordinary animals. Man knows not why a cow, dog, or lion was not born with a brain on a par with ours; why such animals cannot add, subtract, or obtain from books and schooling, that paramount position which Man Holds today.

From *Gadsby*, by Ernest Vincent Wright

# Where the keywords come from

# Where the keywords come from



# Where the keywords come from

- 1 Airbag
- 2 Paranoid Android
- 3 Subterranean Homesick Alien
- 4 Exit Music (For a Film)
- 5 Let Down
- 6 Karma Police
- 7 Fitter Happier
- 8 Electioneering
- 9 Climbing Up the Walls
- 10 No Surprises
- 11 Lucky
- 12 The Tourist

# Advantages and drawbacks

- Stronger than a monoalphabetic cipher.
- Unbreakable with simple frequency analysis.

# Advantages and drawbacks

- Stronger than a monoalphabetic cipher.
- Unbreakable with simple frequency analysis.
- Too time-consuming in practise.
- Periodicity induced by repetitions of the key.
- Breakable using the periodicity and frequency analysis.