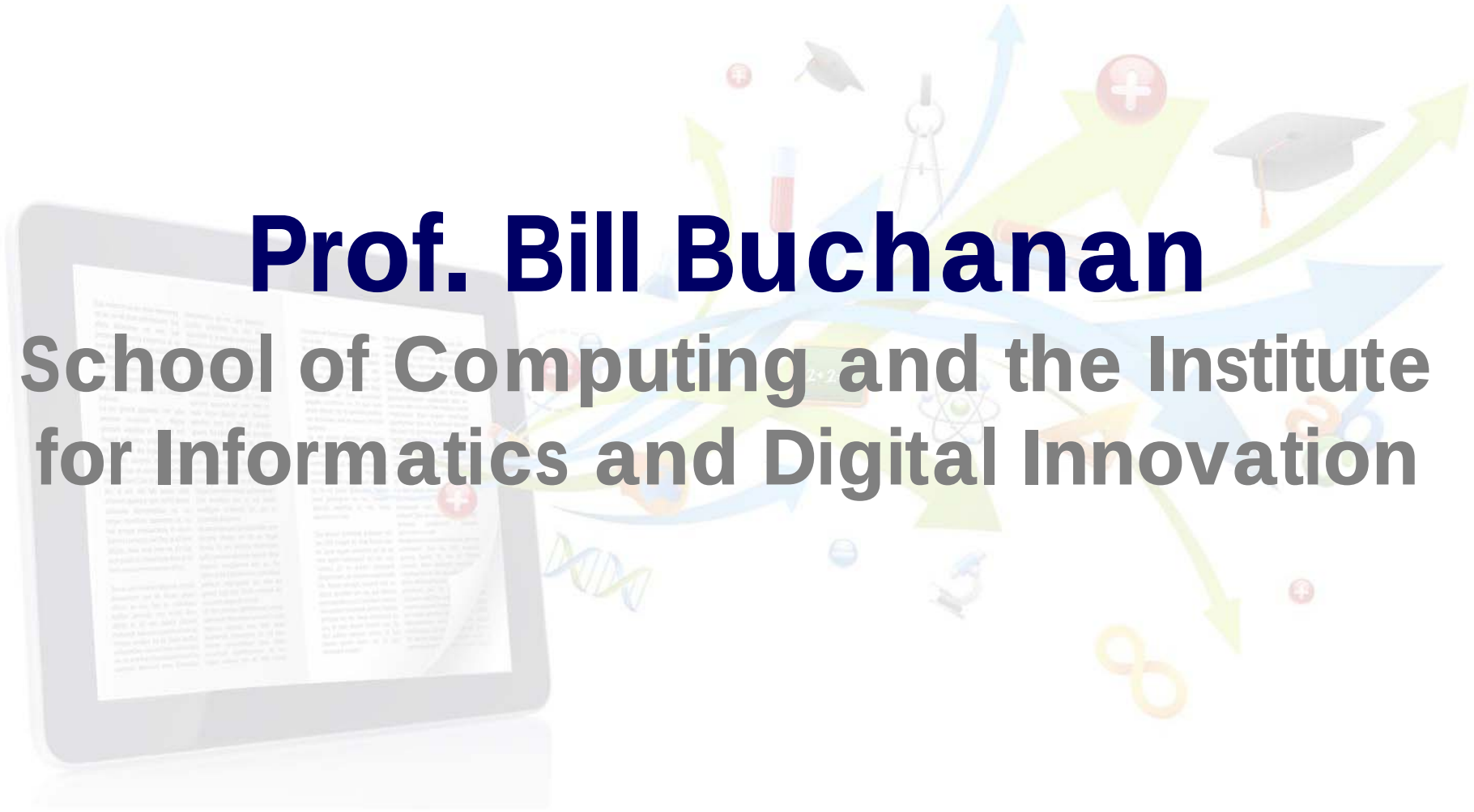


Prof. Bill Buchanan

School of Computing and the Institute for Informatics and Digital Innovation

{CONNECT} HOLYROOD

Thank you for attending

Breakout A

Puzzles, Codes and Cracking: Creating Fun Links between Schools and Universities

#Ltt2013

{CONNECT} HOLYROOD

Edinburgh Napier UNIVERSITY

Puzzles, Codes and Cracking: Creating Fun Links between Schools and Universities

Engaging with Cyber Security ...

Prof Bill Buchanan

Edinburgh Napier UNIVERSITY

... am emailing firstly to express my thanks and delight that this event is taking place. There is a woeful lack of interesting events aimed at Scottish Computing pupils so it is great to see the Cyber lecture.

Prof Bill Buchanan

Edinburgh Napier UNIVERSITY

Large demand for IT graduates

We architecture, we design, we analyse, we build, and we test

Why Computing?

There's lots of different jobs

- Networking.
- Security.
- Software Development.
- Media Design
- Mobile Devices
- Web Development.

New areas every day ...

- Cloud Computing.
- Big Data.
- Mobile Devices.

Edinburgh Napier UNIVERSITY

Data increases every day:

- 12TB of Tweets.
- 90% of all data in the Cloud produced in the last two years.
- 2,500,000,000,000,000 bytes of data produced every data 2.5 Quintillion Bytes – 1 billion hard disks

It's part of every aspect of our lives...

Why Computing?

Everything Is dependent on the Internet

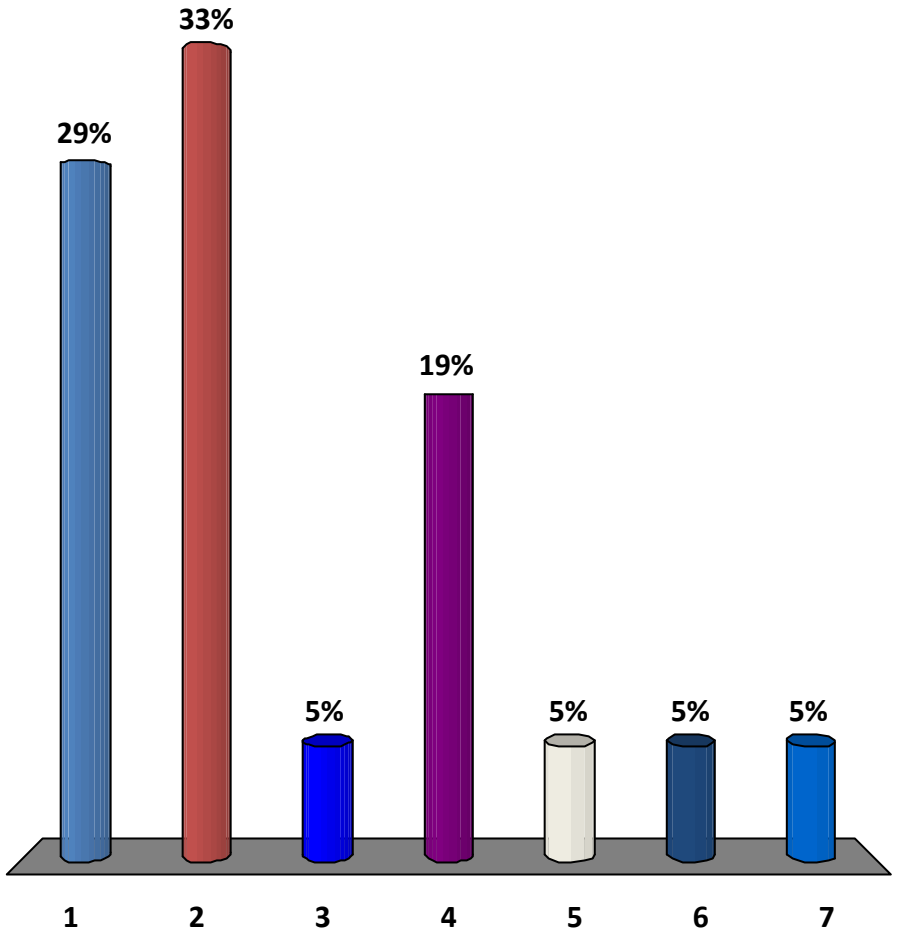
- Banking.
- Oil and Gas.
- E-Commerce.
- Transport.
- … virtually everthing

It's all going digital:

- Data.
- Voice.
- Video.
- Sensors.

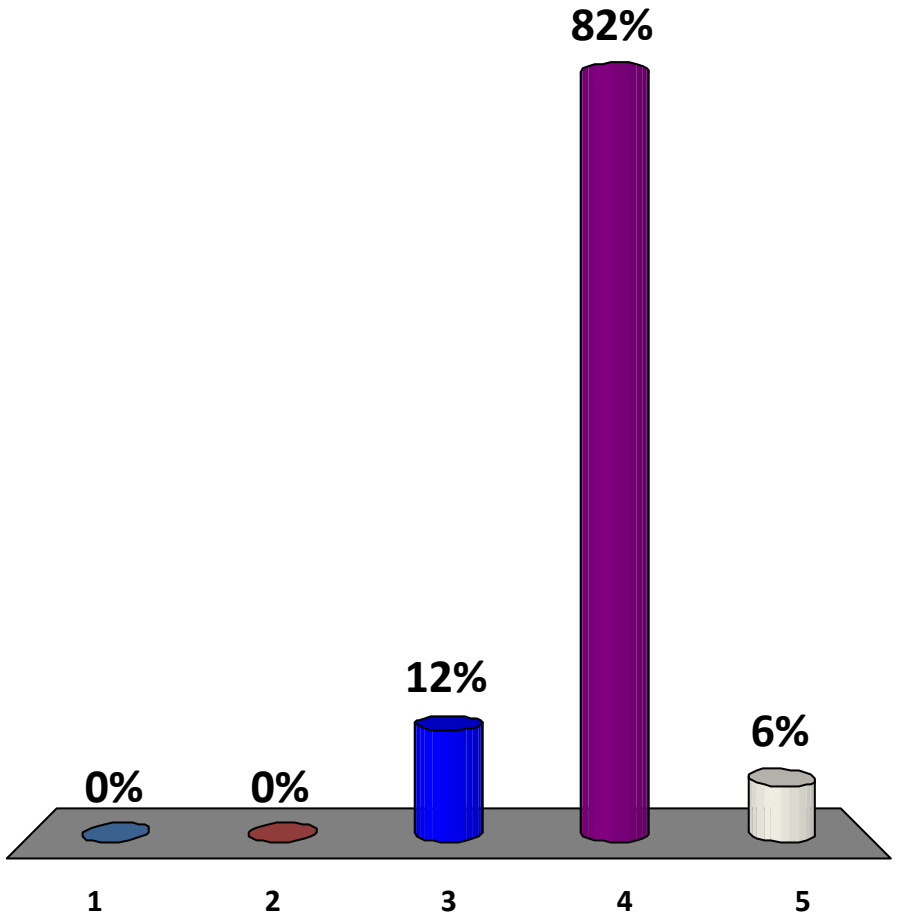
Where are you from?

1. Lothian/Edinburgh.
2. West of Scotland/Glasgow.
3. Fife/Tayside/Dundee.
4. North of Scotland/Aberdeen.
5. Borders/Highlands.
6. England.
7. Somewhere else.



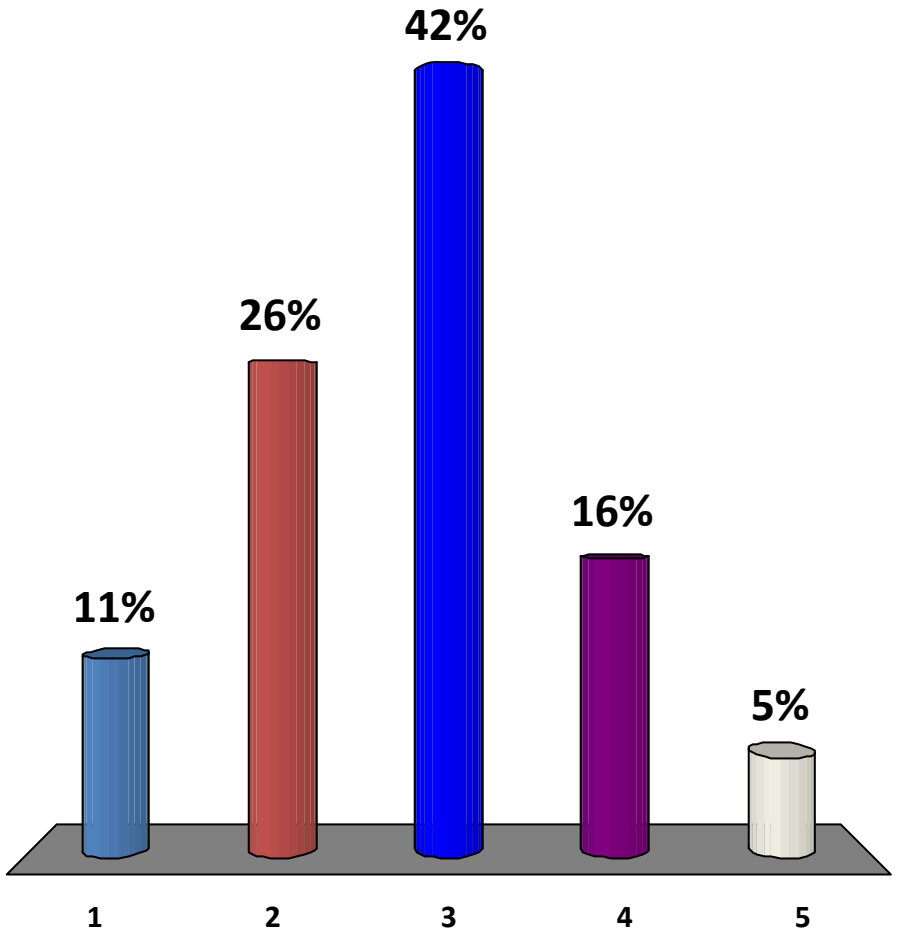
Normally, how long does a BEng (Hons) take in Scotland:

1. 1 Year.
2. 2 Years.
3. 3 Years.
4. 4 Years.
5. 5 Years.



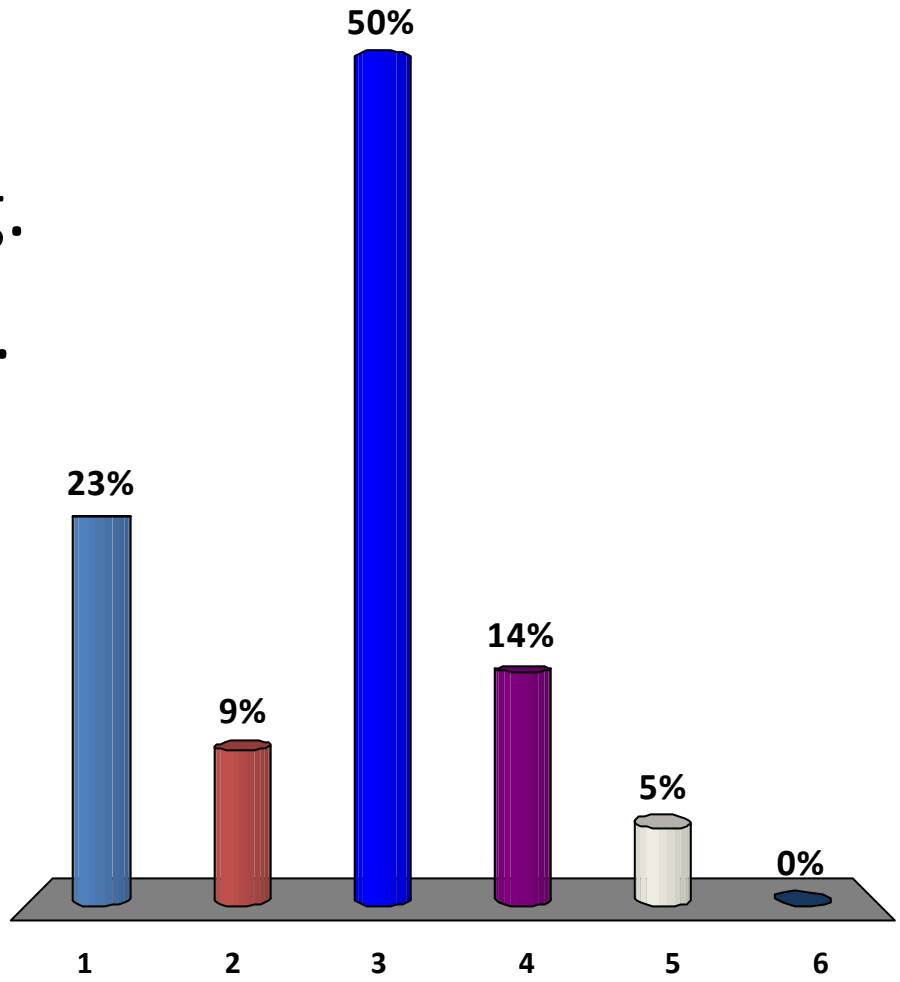
Approx, how many 1st year computing students do we (Edinburgh Napier) take on?

1. 50
2. 150
3. 250
4. 400
5. 650



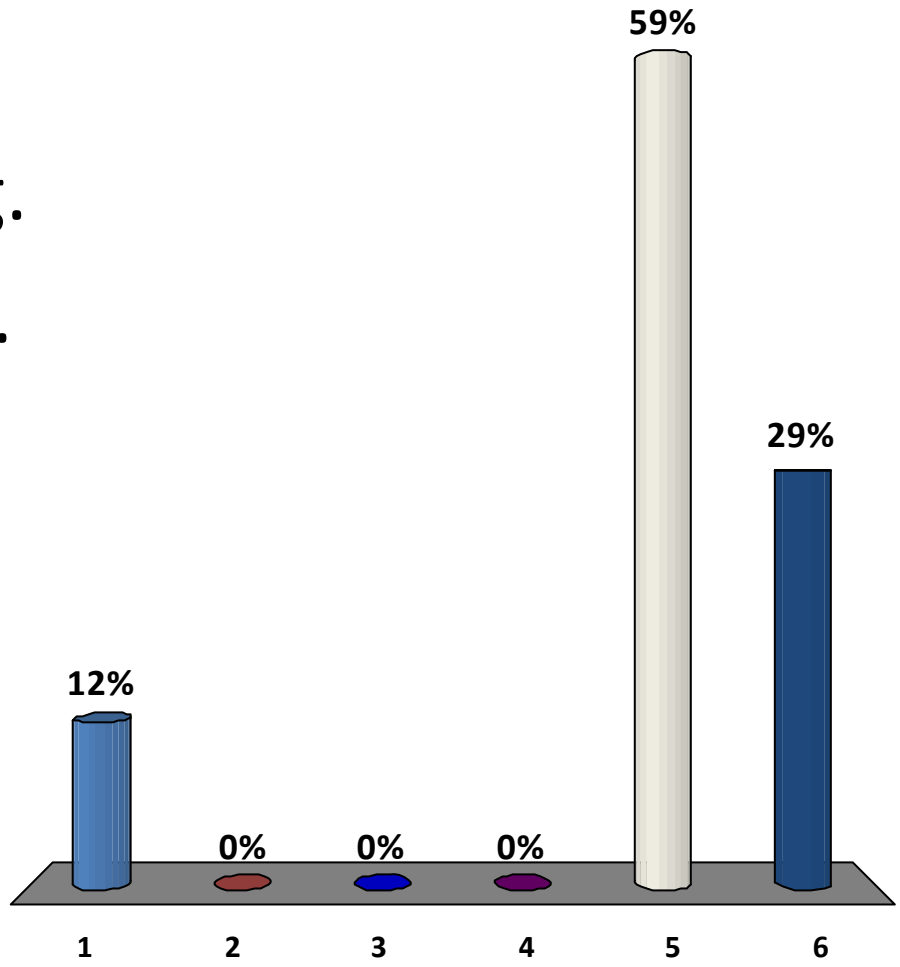
Which programme currently has the most number of students on our undergraduate provision?

1. Digital Media.
2. Software Engineering.
3. Games Development.
4. Security and Digital Forensics.
5. Business Information Systems.
6. Computer Networks.



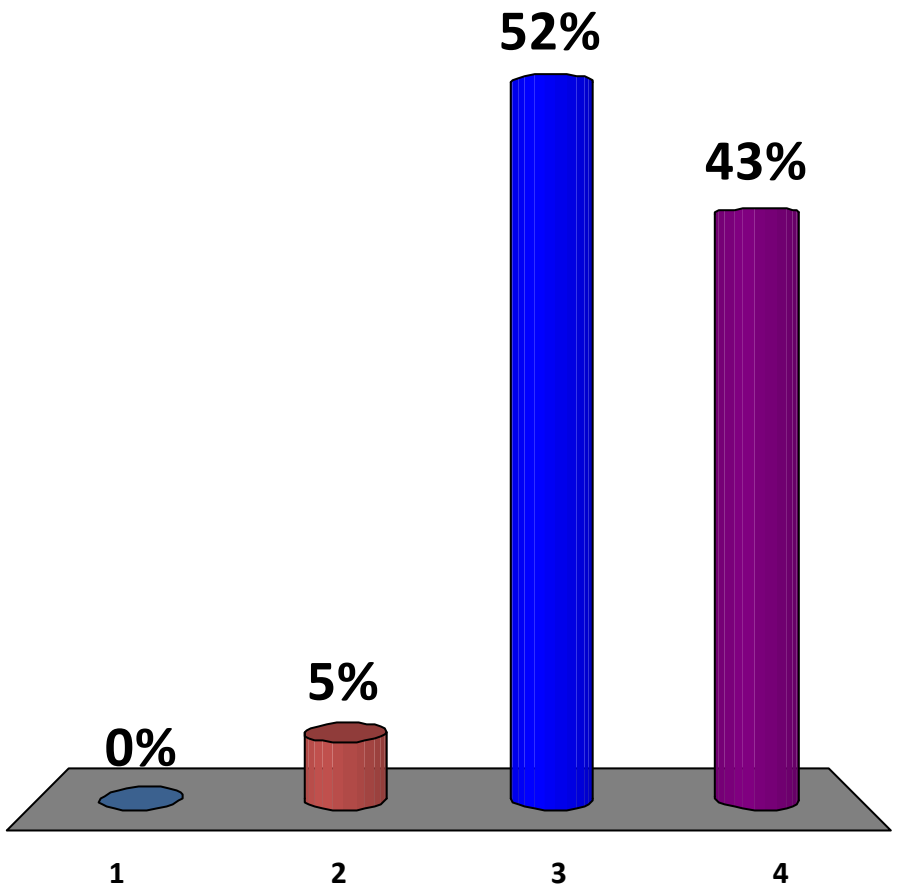
Which programme currently has the least number of students on our undergraduate provision?

1. Digital Media.
2. Software Engineering.
3. Games Development.
4. Security and Digital Forensics.
5. Business Information Systems.
6. Computer Networks.



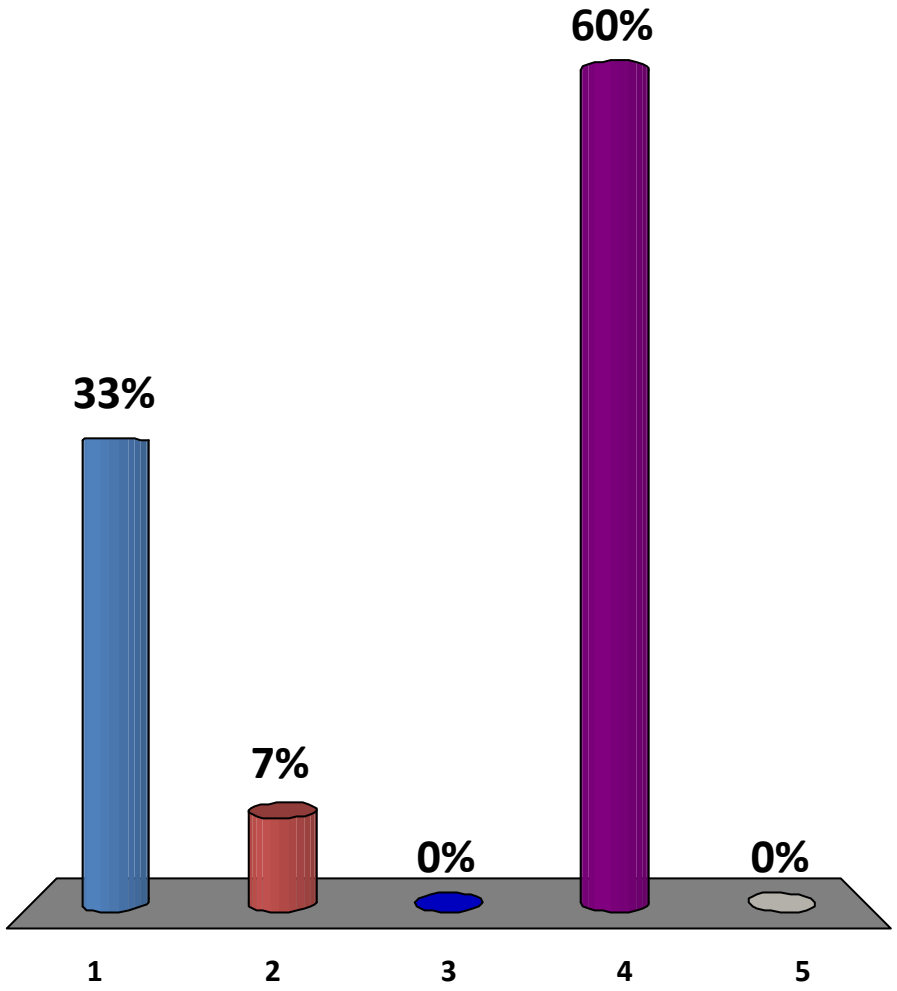
How well do you think that pupils know what jobs there are for them in Computing?

1. Very well.
2. Have a good knowledge of the jobs.
3. Have some knowledge.
4. Have very little knowledge.



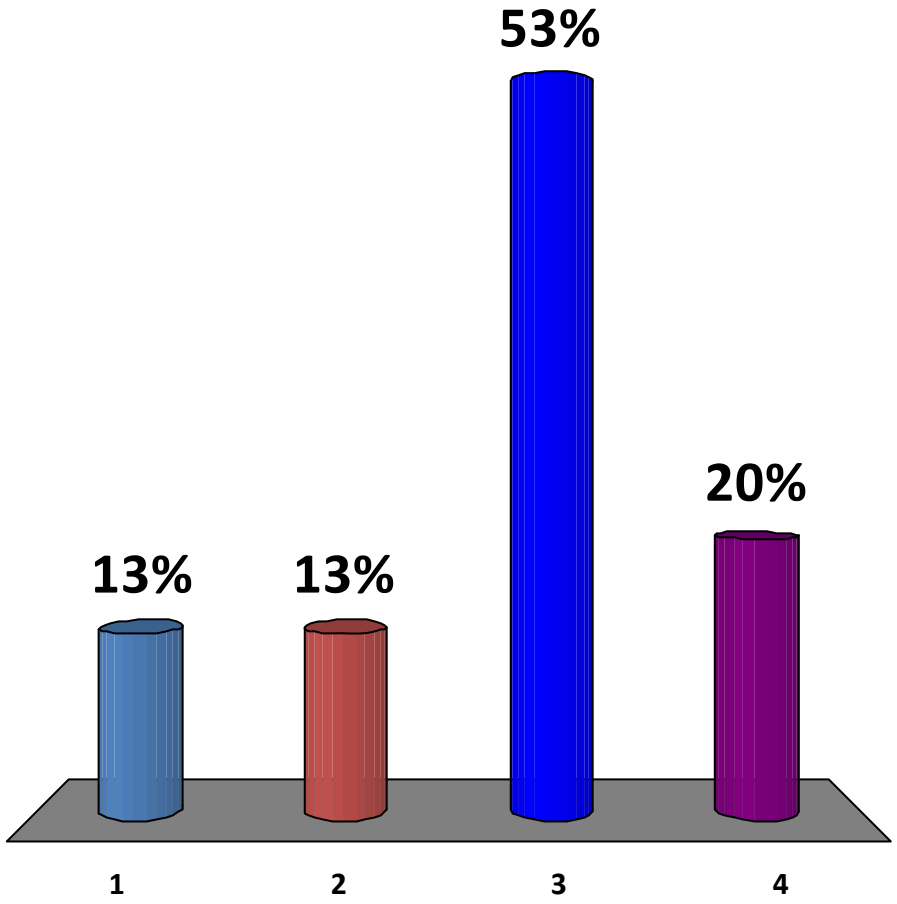
Which area of computing most interests pupils?

1. Computer games.
2. Artificial Intelligence.
3. Computer Networks.
4. Cybercrime and Computer Security.
5. Business IT.



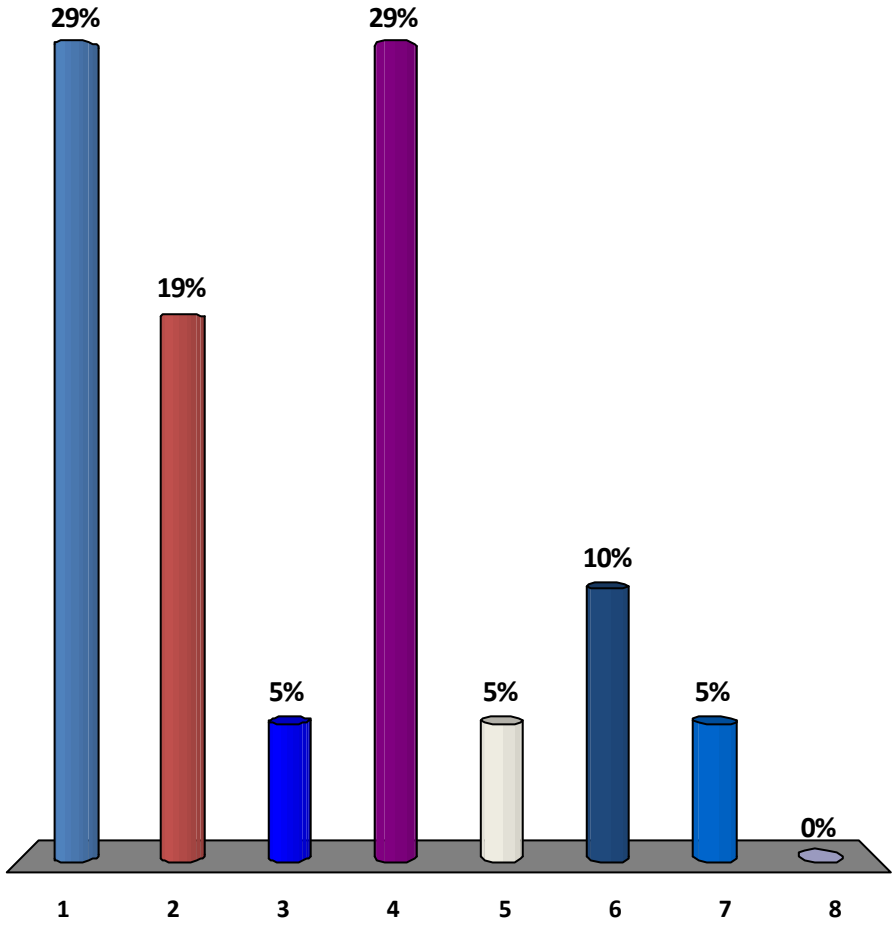
How good is your interface with Computing Schools at Universities:

1. Very good.
2. Fairly good.
3. Limited.
4. Non existent.



What influences a child most in their career choice:

1. Parents.
2. Good teachers.
3. Good jobs.
4. Potential salaries.
5. Careers advice.
6. Good role models.
7. Their peers.
8. Media Pressure



Edinburgh Napier UNIVERSITY

School of Computing

Security and Digital Forensics

Meet the Cast ...

Meet the Cast ...

Eve

Intruder

Bob

Alice

Trent

Trusted third party

Meet the Cast ...

Jake Davis, Shetland Islands

Gary McKinnon

Lulzsec

Eve

Intruder

Bob

Alice

Trent

Trusted third party

Edinburgh Napier UNIVERSITY

Areas:

- Networks.
- Operating Systems.
- People/Motivations.
- Application Software.
- Encryption/Identity.
- Mobile Devices.
- Wireless ...

It's about understanding everything ...

Computer Security and Digital Forensics

Every changing field

- New applications.
- New threats.
- Cloud and Mobility makes it an every great challenge.
- Lots of opportunities for different careers.

It's all going digital:

- Banking.
- On-line shopping.
- Media/News.
- Government.
- Health.

Edinburgh Napier UNIVERSITY

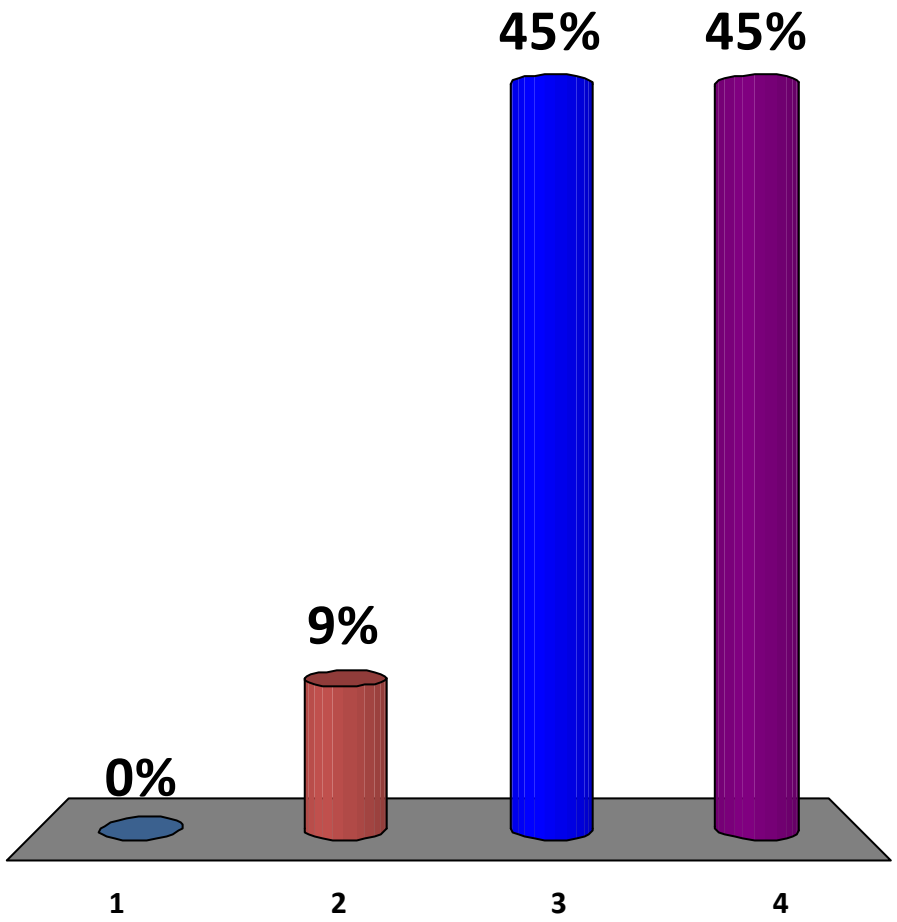
School of Computing

Security and Digital Forensics

… and so to you …

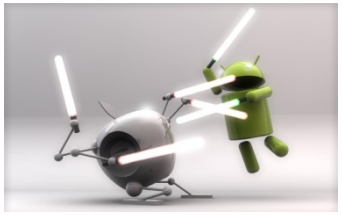
How many hours a day (on average) do you use the Internet?

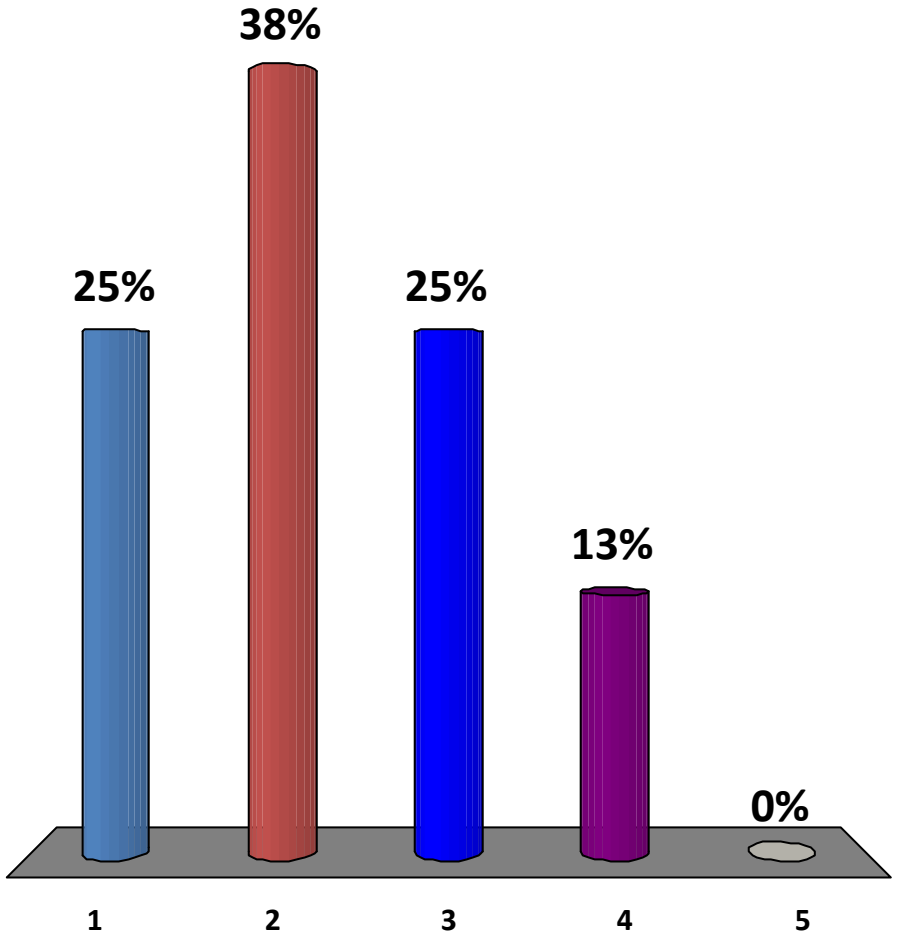
1. Not at all.
2. Less than one hour.
3. Between 1 and 3 hours.
4. More than 3 hours a day.



What type of phone operating system do you have?

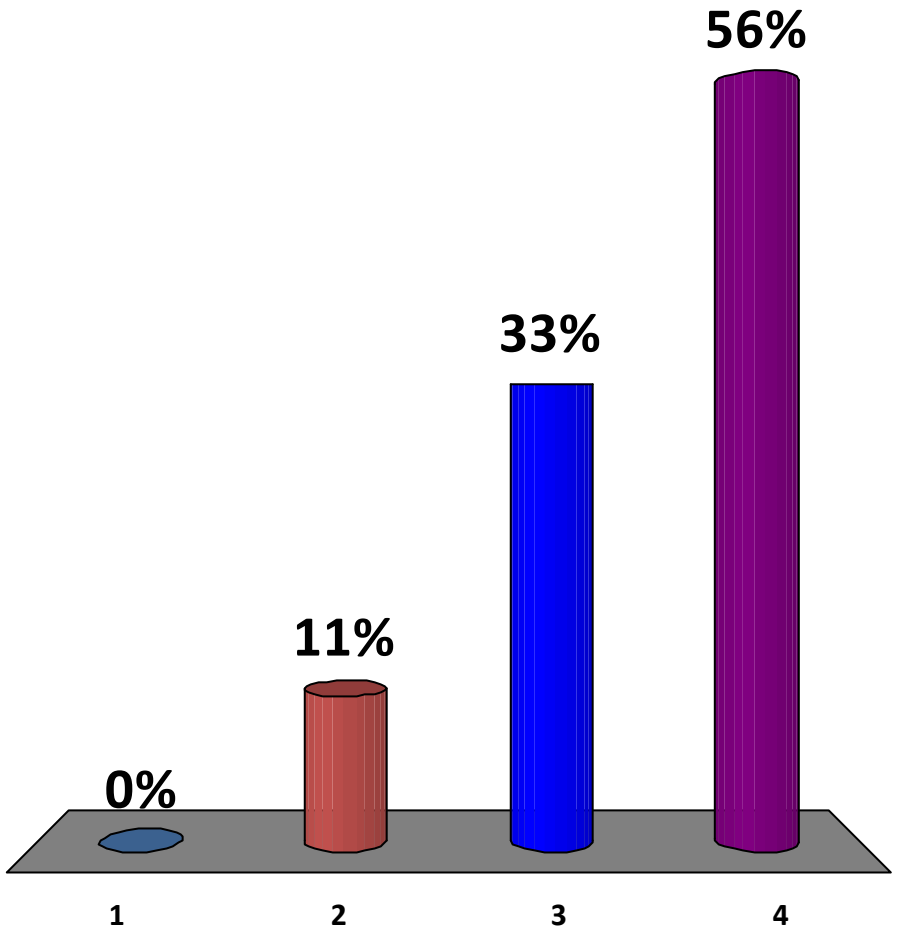
1. Blackberry.
2. Android IOS.
3. Apple IOS.
4. Windows 8.
5. None. I don't have a phone.





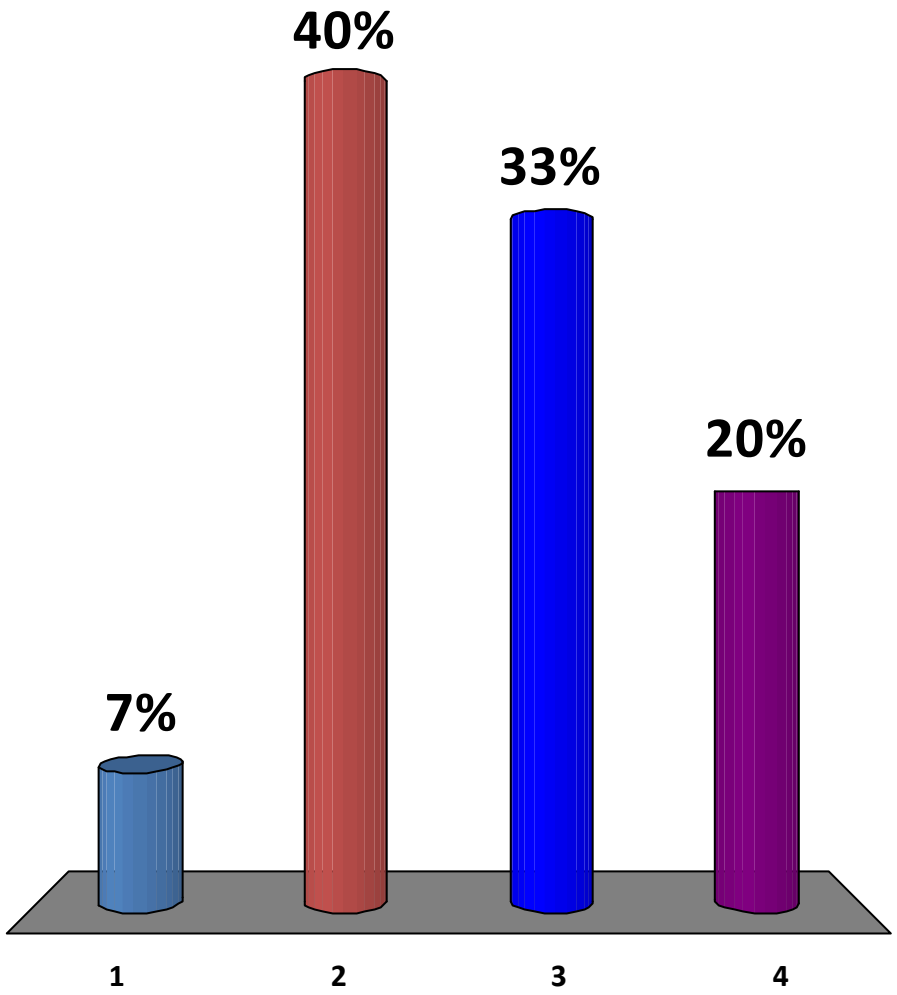
How many different logins do you have:

1. One
2. 2-4.
3. 4-8.
4. More than eight.



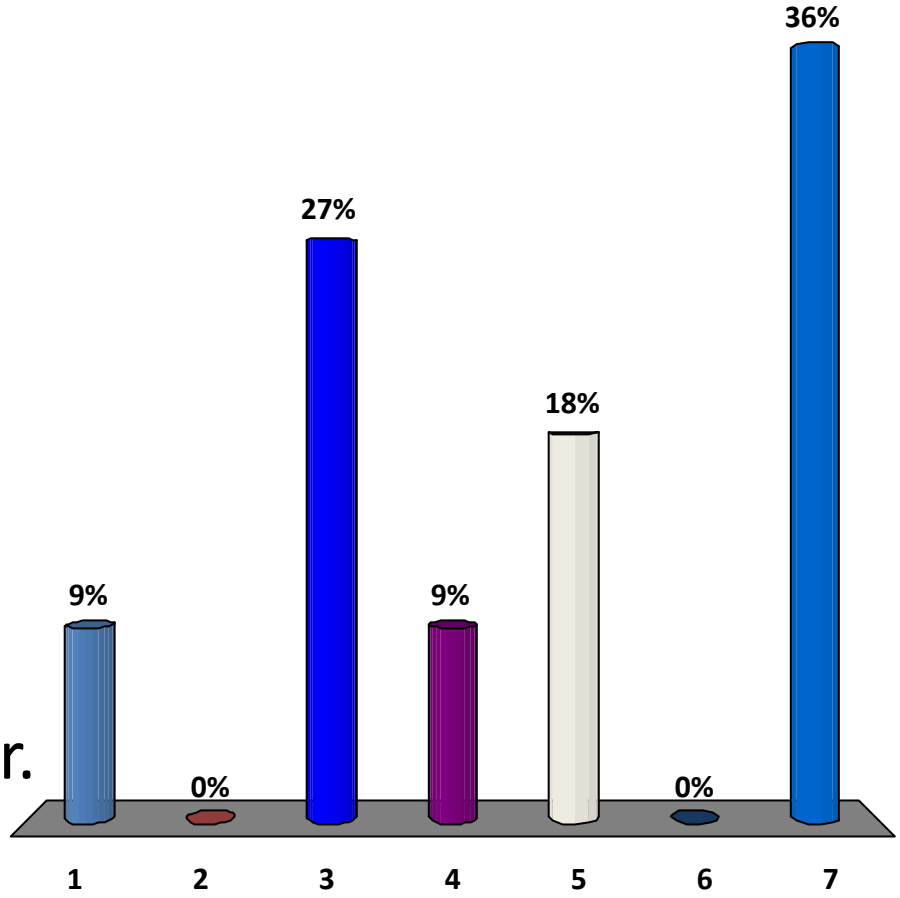
How many different passwords do you have?

1. One
2. 2-4.
3. 4-8.
4. More than eight.



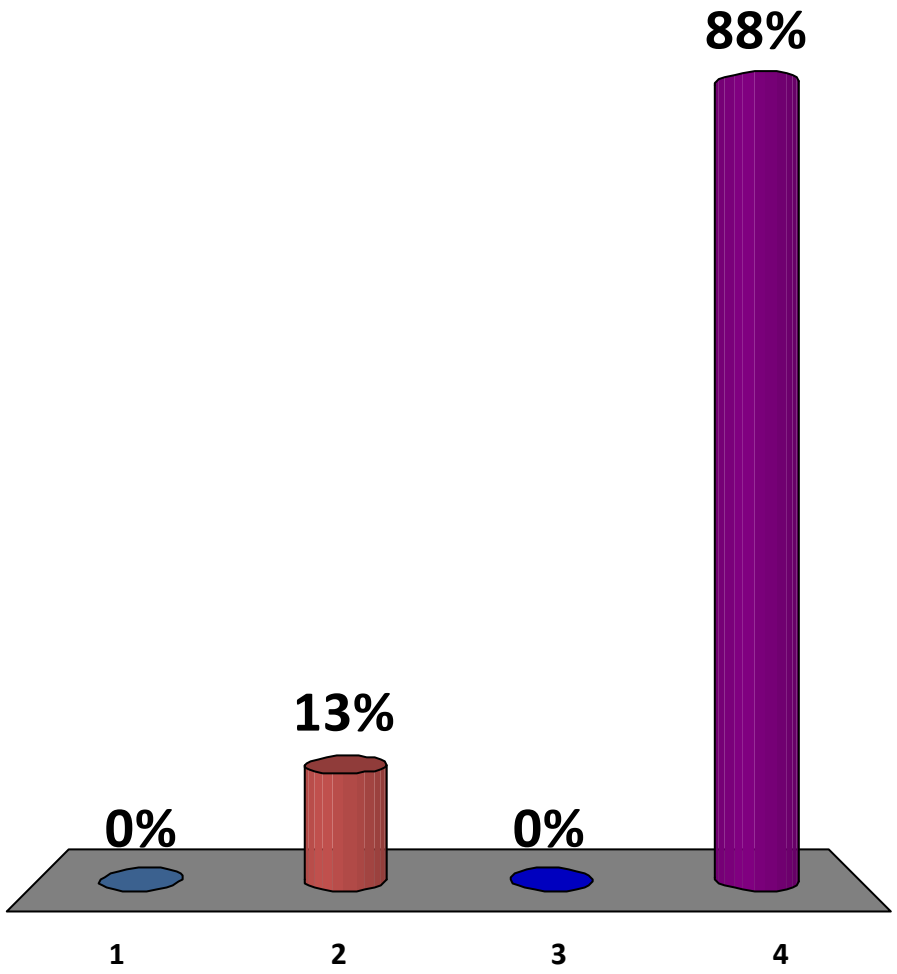
Which best matches your one of your passwords:

1. It is an animal/pet (past/present)
2. It is a car (past/present)
3. It is someone in my family.
4. It is my football/sports team.
5. It is a place.
6. It is a toy/game character.
7. None of the above.



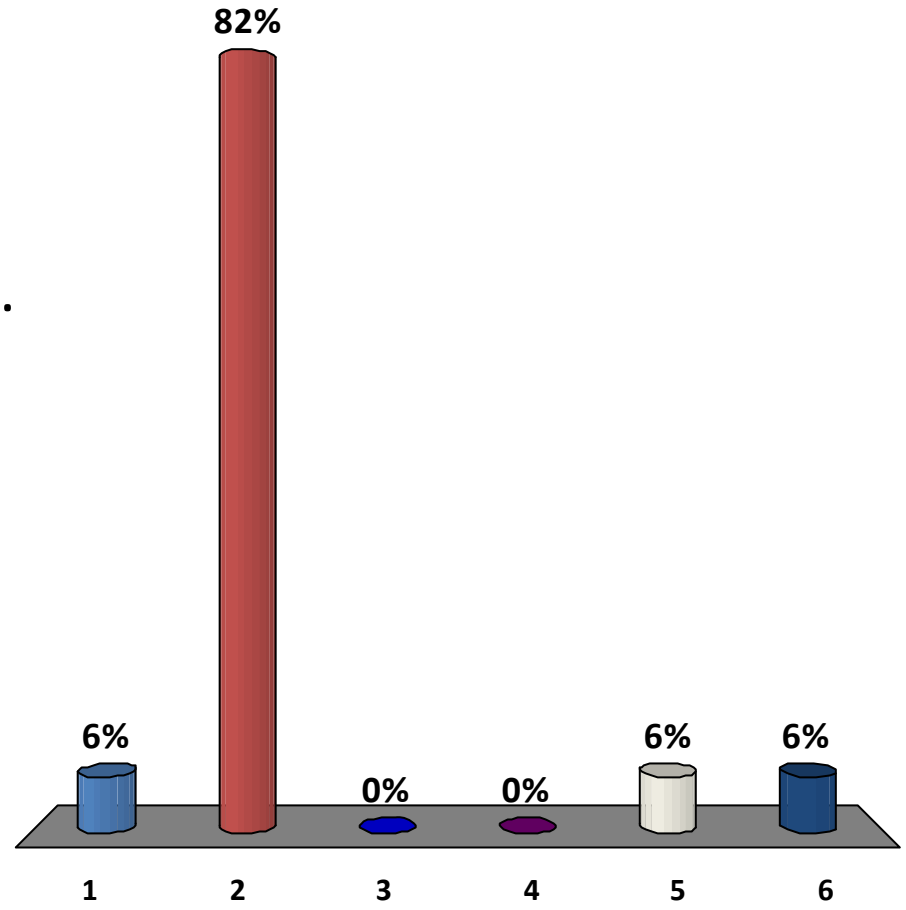
What is your longest password:

1. Up to 7 characters.
2. 8 characters.
3. 9 characters.
4. More than 9 characters.



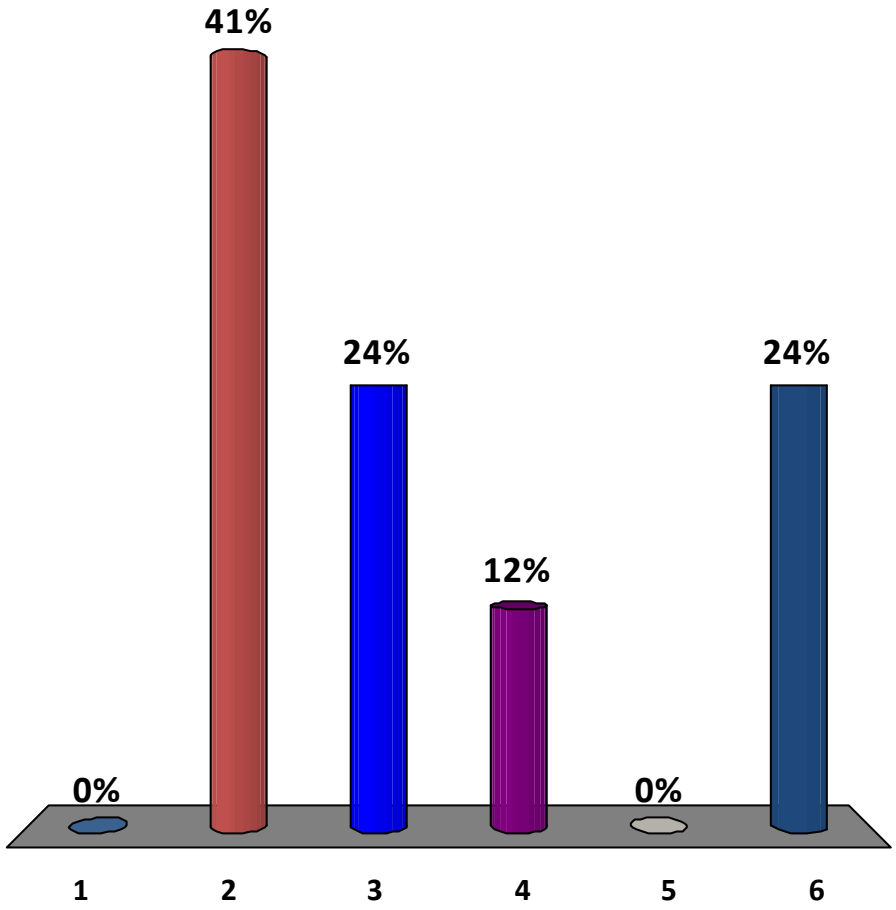
What is your greatest worry on the Internet?

1. Someone steals my identity.
2. Someone gets my bank account/credit card details.
3. Someone tracks my location.
4. Someone gets into my computer.
5. Someone tracks my Web activity.
6. Someone gets my passwords.



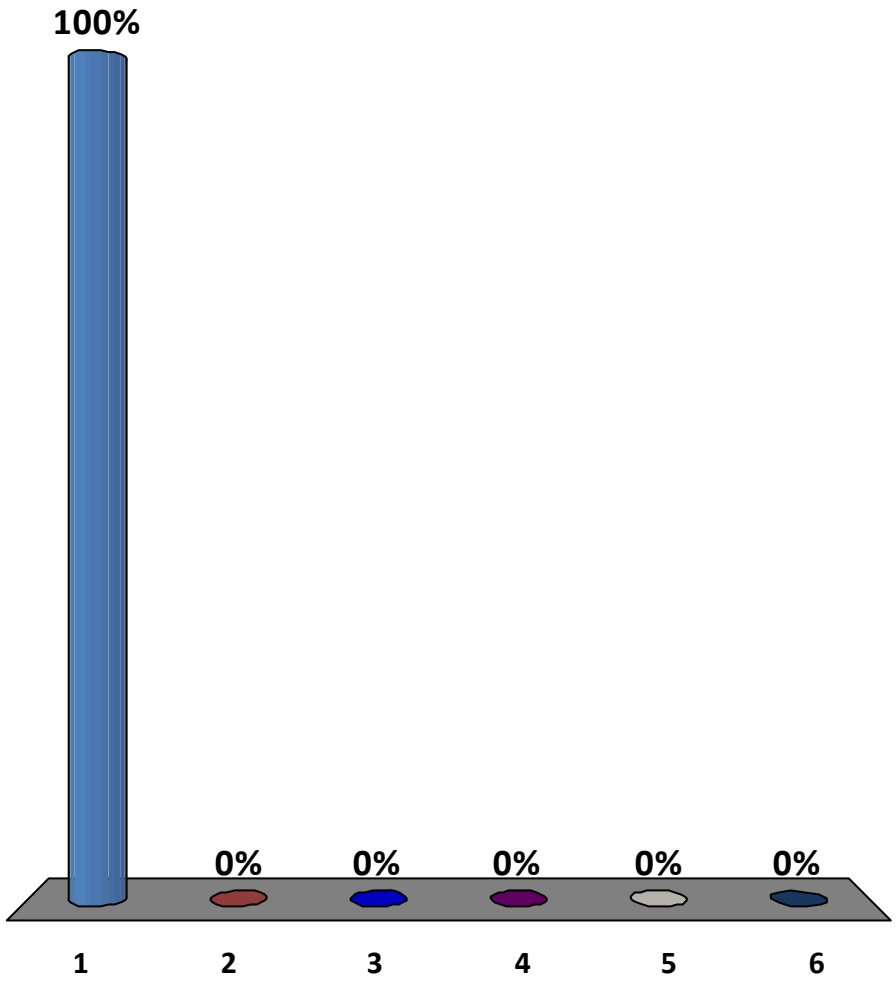
If you had one ID, would you trust most to store it:

1. Facebook.
2. Microsoft.
3. Google.
4. Linkedin.
5. Twitter.
6. Apple.



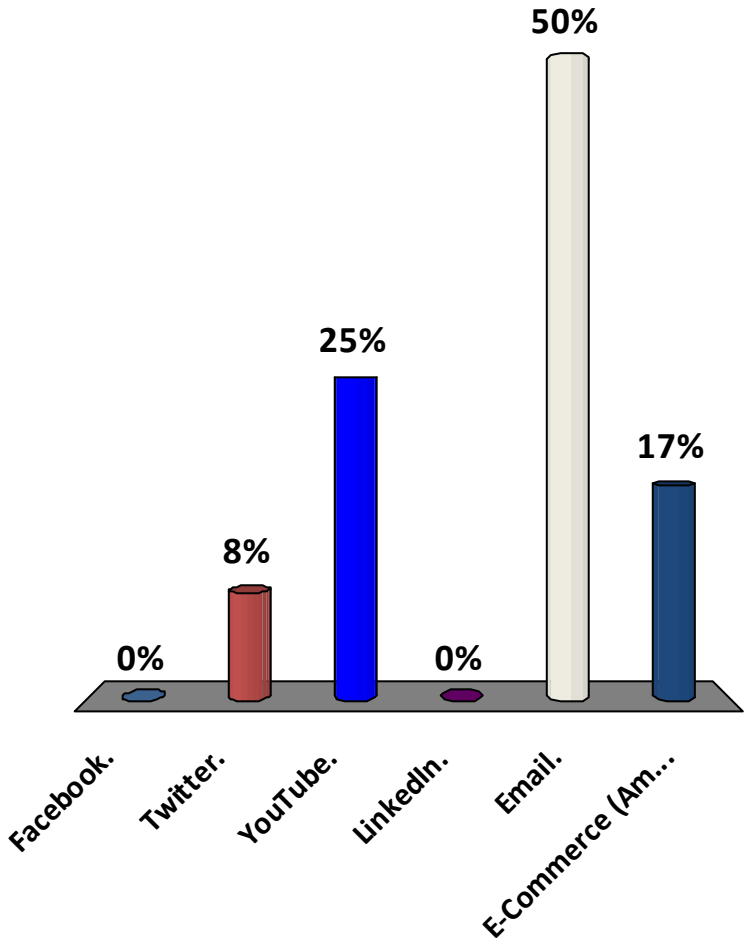
If you had one ID, would you trust least to store it:

1. Facebook.
2. Microsoft.
3. Google.
4. Linkedin.
5. Twitter.
6. Apple.



Which is your favourite application of the Internet?

1. Facebook.
2. Twitter.
3. YouTube.
4. LinkedIn.
5. Email.
6. E-Commerce (Amazon)



Edinburgh Napier UNIVERSITY

Tech Companies

It's part of most companies ...

Why Computing?

Finance Industry

... and lots of others

Edinburgh Napier UNIVERSITY

School of Computing

Security and Digital Forensics

… some codes and puzzles …

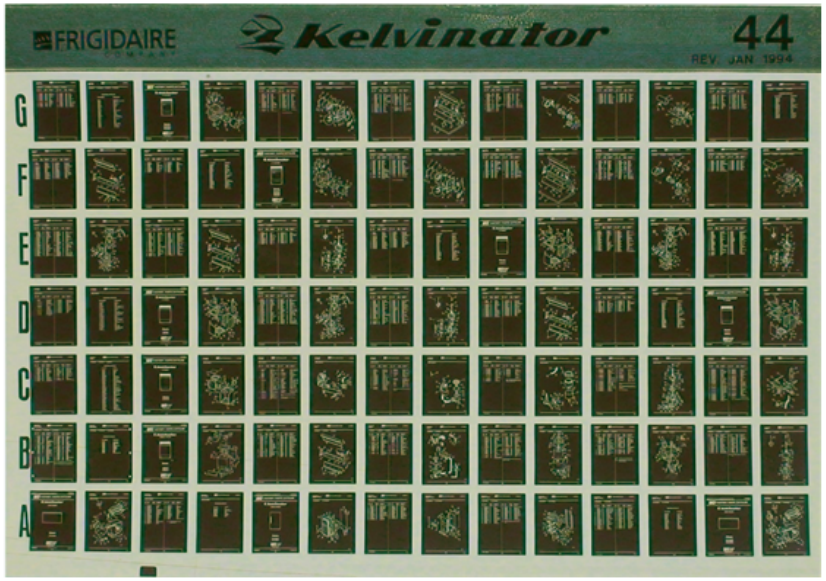
Some old codes

Quilt codes

Flying geese

Sailboat

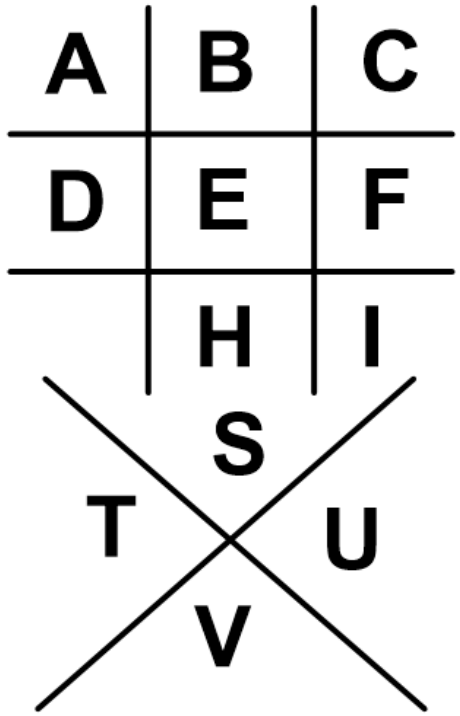
Smoke signals

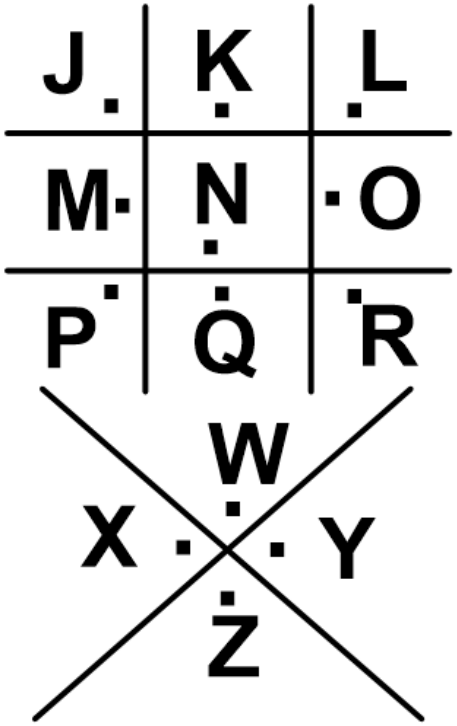


Microfiche

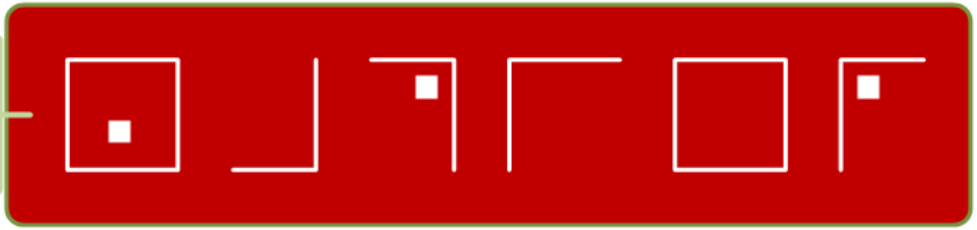
Navajo Code Talkers

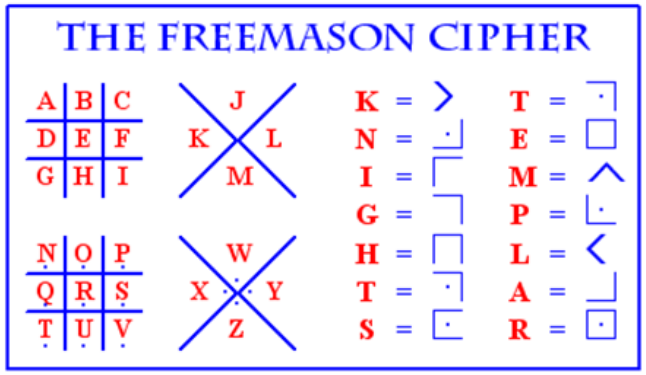
Pigpen





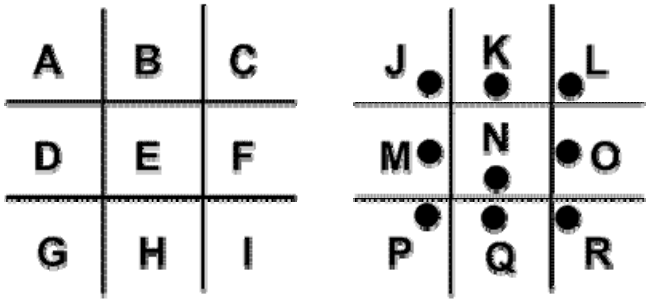
Headstone of James Leeson (1792)

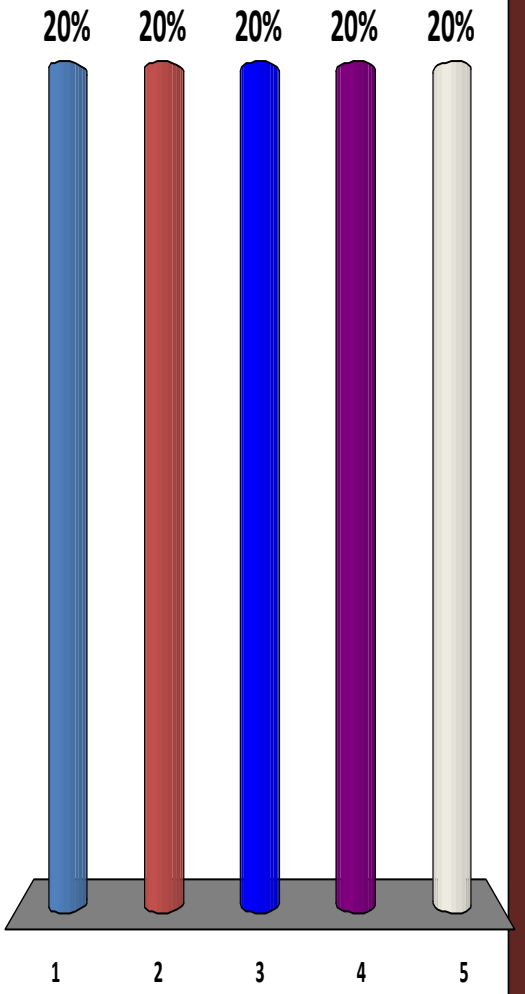




Which word is the following?

1. IGLOOS.
2. HELPER.
3. FOLLOW.
4. INKWELL.
5. RAZORS.





Polybius

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

H	E	L	L	O
23	15	32	32	35

Polybius (Greek historian, ~200BC)

Morse Code

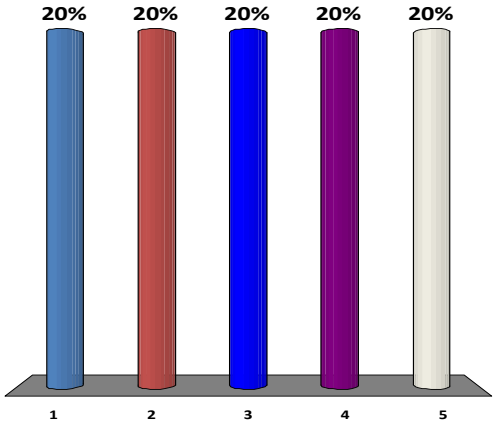
A	(·–)	B	(–···)	C	(–·–·)	D	(–··)
E	(·)	F	(··–·)	G	(– –·)	H	(····)
I	(··)	J	(·– – –)	K	(–·–)	L	(·–··)
M	(– –)	N	(–·)	O	(– – –)	P	(·– –·)
Q	(– –·–)	R	(·–·)	S	(···)	T	(–)
U	(··–)	V	(···–)	W	(·– –)	X	(–··–)
Y	(–·– –)	Z	(– –··)				

Plaintext h e l l o e v e r y o n e

Morse: .... . .-.. .-.. --- . ...- . .-. -.-- --- -. .

What is (···) (— —) (··) (·—··) (·)

1. smell
2. smile
3. sinks
4. slime



International Morse Code

- 1 dash = 3 dots.
- The space between parts of the same letter = 1 dot.
- The space between letters = 3 dots.
- The space between words = 7 dots.

A	·—	V	···—
B	—···	W	·——
C	—·—·	X	—··—
D	—··	Y	—·——
E	·	Z	——··
F	··—·	.	·—·—·—
G	——·	,	——··——
H	····	?	··——··
I	··	/	—··—·
J	·———	@	·——·—·
K	—·—	1	·————
L	·—··	2	··———
M	——	3	···——
N	—·	4	····—
O	———	5	·····
P	·——·	6	—····
Q	——·—	7	——···
R	·—·	8	———··
S	···	9	————·
T	—	0	—————
U	··—		

ADFGVX

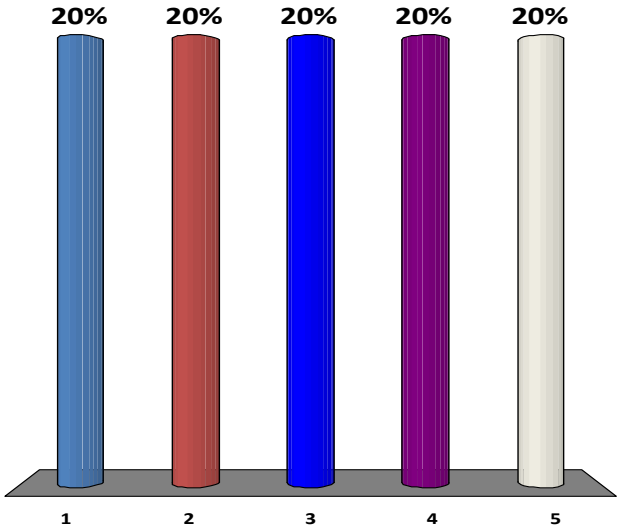
	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Invented by Fritz Nebel, in WW1

FD VG VV FD FG DV DA AG XF

What is DX DV AD AD XF

1. slips
2. happy
3. ankle
4. cores



	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Caesar Code

Caesar

Mark Antony

Cleopatra

Plaintext

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

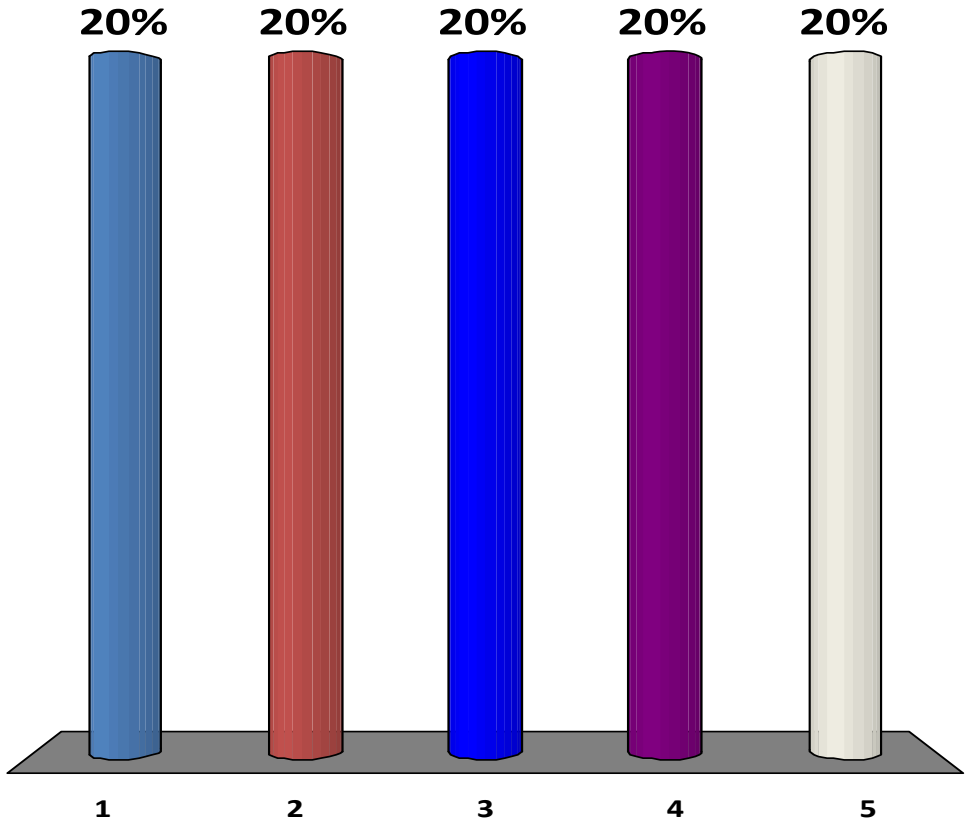
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Ciphertext

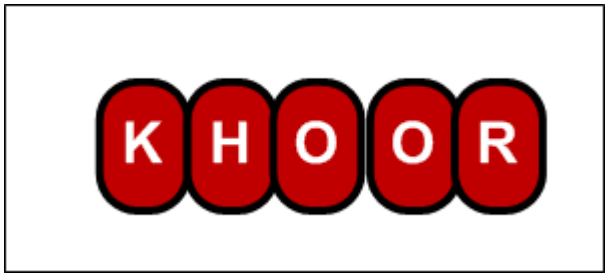
K H O O R

How many codes are possible for a Caesar code

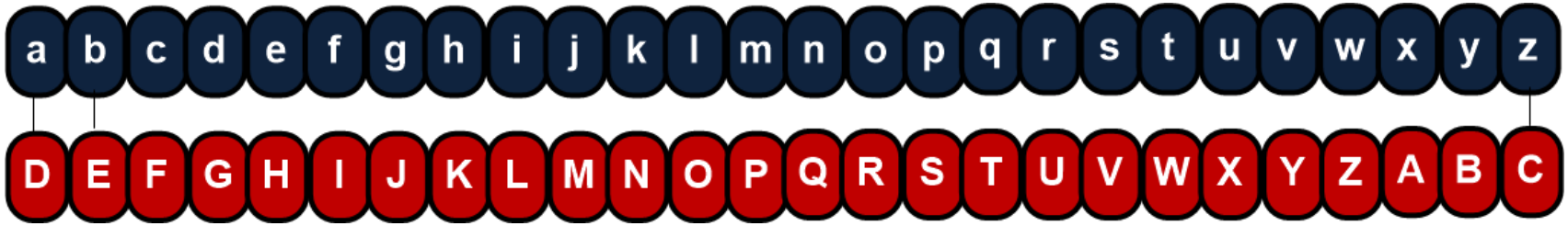
1. 24
2. 25
3. 26
4. 256



With Caeser code, what is the plain text message:



1. apple
2. hello
3. ankle
4. solid



Scrambled

Caesar

Mark Antony

Cleopatra

Plaintext

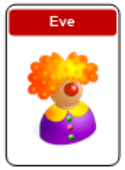
a b c d e f g h i j k l m n o p q r s t u v w x y z

Ciphertext

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

L Q N Z D O O

Scottish Christmas Cyber Lecture 2012



ONR ECRYAPFJ FDAO PFOXADRT NPM TGOG UGD LR RDUCIEORT JP ONGO AO UGDDPO LR YARMRT LI GDIPDR ONGO AO MGJ DPO ADORDTRT QCPK. MAON ECAYGOR-SRI RDUCIEOAPD, LPL GDT GXAUR FJR ONR JGKR JRUCRO SRI OP RDUCIEO GDT TRUCIEO ONR KRJJGZR. ONRD, FJADZ G SRI ADORCUNGDZR KRONPT JFUN GJ TAQQAR-NRXXKGD, LPL GDT GXAUR UGD ZRDRCGOR ONR JGKR JRUCRO SRI, RYRD AQ RYR AJ XAJORDADZ OP ONRAC UPKKFDAUGOAPDJ. MAON EFLXAU-SRI RDUCIEOAPD, LPL GDT GXAUR TP DPO NGYR ONR JGKR ECPLXRK, GJ GXAUR UGD GTYRCOAJR NRC EFLXAU SRI JP ONGO LPL UGD FJR AO OP RDUCIEO UPKKFDAUGOAPDJ OP NRC. ONR PDXI SRI ONGO UGD TRUCIEO ONR UPKKFDAUGOAPDJ AJ GXAUR'J ECAYGOR SRI (MNAUN, NPERQFXXI, RYR UGDDPO ZRO NPXT PQQ). MR DPM, ONPFZN, NGYR QPFC QFCONRC ECPLXRKJ:- NPM TP MR SDPM ONGO AO MGJ CRGXXI LPL MNP JRDO ONR TGOG, GJ GDIPDR UGD ZRO GXAUR'J EFLXAU SRI, GDT ONFJ ECRORDT OP LR LPL? - NPM UGD MR ORXX ONGO ONR KRJJGZR NGJ DPO LRRD OGKERCRT MAON? - NPM TPRJ LPL TAJOCALFOR NAJ EFLXAU SRI OP GXAUR, MAONPFO NGYADZ OP EPJO AO PDOP G MRL JAOR PC QPC LPL OP LR PD-XADR MNRD GXAUR CRGTJ ONR KRJJGZR? - MNP UGD MR CRGXXI OCFJO OP ECPERCXI GFONRDOAUGOR LPL? PLYAPFJXI MR UGD'O OCFJO LPL OP GFONRDOAUGOR ONGO NR CRGXXI AJ LPL. ONRJR WFRJOAPDJ MAXX LR GDJMRCRT AD ONAJ FDAO, GJ MR MAXX XPPS GO ONR FJGZR PQ NGJNADZ OP QADZRC-ECADO TGOG, GDT ONRD NPM LPL'J ECAYGOR SRI UGD LR FJRT OP GFONRDOAUGOR NAKJRXQ. QADGXXI, AO MAXX XPPS GO ONR MGI ONGO G EFLXAU SRI UGD LR TAJOCALFORT, FJAD TAZAOGX URCOAQAUGORJ, MNAUN UGD UGCCI RDUC SRI. ONAJ UNGEORC MAXX JNPM ONR AKEPCOGDUR P GFONRDOAUGOAPD GDT GJJFCGDUR, GXPDZ MAON UPDQATRDOAGXAOI (QAZFCR 4.1), GDT ONR FJGZR PC LAPKROCAUJ.

Letters (%)		Digrams (%)		Trigrams (%)		Words (%)	
E	13.05	TH	3.16	THE	4.72	THE	6.42
T	9.02	IN	1.54	ING	1.42	OF	4.02
O	8.21	ER	1.33	AND	1.13	AND	3.15
A	7.81	RE	1.30	ION	1.00	TO	2.36
N	7.28	AN	1.08	ENT	0.98	A	2.09
I	6.77	HE	1.08	FOR	0.76	IN	1.77
R	6.64	AR	1.02	TIO	0.75	THAT	1.25
S	6.46	EN	1.02	ERE	0.69	IS	1.03
H	5.85	TI	1.02	HER	0.68	I	0.94
D	4.11	TE	0.98	ATE	0.66	IT	0.93
L	3.60	AT	0.88	VER	0.63	FOR	0.77
C	2.93	ON	0.84	TER	0.62	AS	0.76
F	2.88	HA	0.84	THA	0.62	WITH	0.76
U	2.77	OU	0.72	ATI	0.59	WAS	0.72
M	2.62	IT	0.71	HAT	0.55	HIS	0.71
P	2.15	ES	0.69	ERS	0.54	HE	0.71
Y	1.51	ST	0.68	HIS	0.52	BE	0.63
W	1.49	OR	0.68	RES	0.50	NOT	0.61
G	1.39	NT	0.67	ILL	0.47	BY	0.57
B	1.28	HI	0.66	ARE	0.46	BUT	0.56
V	1.00	EA	0.64	CON	0.45	HAVE	0.55
K	0.42	VE	0.64	NCE	0.43	YOU	0.55
X	0.30	CO	0.59	ALL	0.44	WHICH	0.53
J	0.23	DE	0.55	EVE	0.44	ARE	0.50
Q	0.14	RA	0.55	ITH	0.44	ON	0.47
Z	0.09	RO	0.55	TED	0.44	OR	0.45

Edinburgh Napier UNIVERSITY

Puzzles, Codes and Cracking: Creating Fun Links between Schools and Universities

Engaging with Cyber Security ...

Prof Bill Buchanan