Activity 2: Generating keys using more realistic large integers

In real-life, encryption used for far larger numbers would be very hard to guess. In Activity 2 we will use more realistic larger numbers.

Drawing up modular tables would take a very long time, so we will use a special mathematical technique, a kind of shortcut for finding modular inverses.

The second 'message' will be an integer corresponding to a three-letter word you will select from the table attached.

Choose your keys

1. Choose a number A between 25 and 50. ☐ **A**

2. Choose a second number B between 25 and 50. ☐ **B**

3. Multiply A and B. Call this number C. ☐ **C**

4. Subtract 1. Call this number D. ☐ **D**

- Your public key is A + B + C ☐ **Public key**
- Your encryption key is A + D. ☐ **Encryption key**
- Your decryption or private key is B + D. ☐ **Decryption key**

Tell all others their public and encryption keys. Your decryption key is kept private!

Now if you took a lot of trouble to check, you would find that:
Encryption key X Decryption key = 1 in the modulus of our Public key.

We are finally ready to **encode** and **decode** our secret message as we have found two numbers whose product is 1 in the modulus of our private key.

Encryption

Choose a message for transmission from the sheet of three letter words attached.

5. Note the number corresponding to your word in the table and multiply it by your **encryption** key

encryption key ☐ **Message (using table at back)** X ☐ **Encryption key** = ☐ **F**

6. Divide **F** by the **public** key and write down only those digits appearing in front of the decimal point. ☐ **G**

7. Multiply **G** by your **public** key. ☐ **H**

8. Subtract **H** from the result in **F** above.
The result is your encrypted secret word. ☐ **I Encrypted message**

Decryption

9. Multiply the encoded message in **I** above by the **decryption** key. ☐ **J**

10. Divide the result in **J** ~~F~~ by the **public** key. Write down write down only those digits appearing in front of the decimal point. ☐ **K**

11. Multiply the result in **K** ~~G~~, by the **public** key ☐ **L**

12. Subtract the result in **L** ~~H~~ from the result in **J** ~~F~~. ☐ **M**

The result is your decrypted message – a number revealing your secret three-letter word, known only to those who have your private **decrypting** key alongside your **public** key.

DIGITAL TECHNOLOGIES HUB

Table of three-letter words

#	Word	#	Word	#	Word	#	Word	#	Word	#	Word
1	ace	49	beg	97	cup	145	ere	193	gig	241	hum
2	act	50	bet	98	cur	146	erg	194	gin	242	hut
3	add	51	bib	99	cut	147	err	195	gnu	243	ice
4	ado	52	bid	100	dab	148	eta	196	gob	244	icy
5	ads	53	big	101	dad	149	eve	197	god	245	ids
6	adz	54	bin	102	dam	150	ewe	198	goo	246	ifs
7	aft	55	bit	103	day	151	eye	199	gos	247	ilk
8	age	56	boa	104	deb	152	fad	200	got	248	ill
9	ago	57	bob	105	den	153	fan	201	gum	249	imp
10	aha	58	bog	106	dew	154	far	202	gun	250	ink
11	aid	59	boo	107	did	155	fat	203	gut	251	inn
12	ail	60	bop	108	die	156	fax	204	guy	252	ins
13	aim	61	bow	109	dig	157	fed	205	gym	253	ion
14	air	62	box	110	dim	158	fee	206	gyp	254	ire
15	alb	63	boy	111	din	159	fen	207	had	255	irk
16	ale	64	brr	112	dip	160	fer	208	hag	256	ism
17	all	65	bud	113	dis	161	few	209	hah	257	its
18	amp	66	bug	114	doc	162	fey	210	ham	258	ivy
19	and	67	bum	115	doe	163	fez	211	has	259	jab
20	ani	68	bun	116	dog	164	fib	212	hat	260	jag
21	ant	69	bur	117	don	165	fie	213	haw	261	jam
22	any	70	bus	118	dos	166	fig	214	hay	262	jar
23	ape	71	but	119	dot	167	fin	215	hem	263	jaw
24	apt	72	buy	120	dry	168	fir	216	hen	264	jay
25	arc	73	bye	121	dub	169	fit	217	hep	265	jet
26	are	74	cab	122	dud	170	fix	218	her	266	jib
27	ark	75	cad	123	due	171	flu	219	hes	267	jig
28	arm	76	cam	124	dug	172	fly	220	hew	268	job
29	art	77	can	125	duh	173	fob	221	hex	269	jog
30	ash	78	cap	126	dun	174	foe	222	hey	270	jot
31	ask	79	car	127	duo	175	fog	223	hid	271	joy
32	asp	80	cat	128	dye	176	fop	224	hie	272	jug
33	ate	81	caw	129	ear	177	for	225	him	273	jut
34	auk	82	chi	130	eat	178	fox	226	hip	274	keg
35	awe	83	cob	131	ebb	179	fro	227	his	275	ken
36	awl	84	cod	132	eel	180	fry	228	hit	276	key
37	axe	85	cog	133	egg	181	fun	229	hob	277	kid
38	aye	86	con	134	ego	182	fur	230	hod	278	kin
39	baa	87	coo	135	eke	183	gab	231	hoe	279	kit
40	bad	88	cop	136	elf	184	gad	232	hog	280	lab
41	bag	89	cot	137	elk	185	gag	233	hop	281	lad
42	bah	90	cow	138	ell	186	gal	234	hos	282	lag
43	ban	91	cox	139	elm	187	gap	235	hot	283	lam
44	bar	92	coy	140	ems	188	gas	236	how	284	lap
45	bat	93	cry	141	emu	189	gee	237	hub	285	law
46	bay	94	cub	142	end	190	gel	238	hue	286	lax
47	bed	95	cud	143	eon	191	gem	239	hug	287	lay
48	bee	96	cue	144	era	192	get	240	huh	288	lea

DIGITAL TECHNOLOGIES HUB