

The World as Cryptogram

Saul-Paul Sirag

International Space Sciences Organization

November 7, 2000

Alan Turing is quoted on the epigram page of the novel *Cryptonomicon*, by Neal Stephenson (Perennial, 1999):

“There is a remarkably close parallel between the problems of the physicist and those of the cryptographer. The system on which a message is enciphered corresponds to the laws of the universe, the intercepted messages to the evidence available, the keys for a day or a message to important constants which have to be determined. The correspondence is very close, but the subject matter of cryptography is very easily dealt with by discrete machinery, physics not so easily.”

Let the “important constant” be 137, the physicist’s favorite number, since it is the inverse of the fine structure constant, and also the magnetic charge number of the Dirac monopole. Richard feynman says that “every good theoretical physicist puts 137 up on his wall and worries about it.”

Let the cryptographic system be the version of public key cryptography due to Rivest, Shamir, and Adleman called the RSA system. It is based on the number theory of prime numbers:

Pick two prime numbers p and q , their product will be the modulus. Then pick an encoding e which will be used as an exponent. There must be a decoding number d , also used as an exponent. There are only three equations describing the system:

$$M^e = C \bmod (p \times q); \quad C^d = M \bmod (p \times q);$$

$$\text{provided that } e \times d = 1 \bmod ((p+1) \times (q+1)).$$

This means, take the message M coded as a binary number (as in any computer); then multiply M by itself e times giving M^e ; now divide M^e by the modulus $p \times q$; and the remainder will be C , the encrypted version of the message (number M). To get the message back, just take C and multiply it by itself d times to get C^d ; and dividing C^d by the modulus $p \times q$ leaves M as the remainder. This is guaranteed to work if the number $e \times d$ when divided by the modulus $((p+1)(q+1))$ leaves 1 as the remainder.

Of course, the security of the system is based on the well known difficulty of factoring large numbers into primes. So in the RSA system p and q and e are all very large numbers, say around a google (or 10^{100}). This makes it very difficult to break $p \times q$ down into its factors p

and q . The modulus $p \times q$ and the encoding number e are made public like a telephone number. But the decoding number d and the factors p and q are kept secret.

When I first read the above RSA equations in a computer magazine called *ROM*, I was at Robert Anton Wilson's house in Berkeley. He had already published his book *Cosmic Trigger* (And/Or, Berkeley, 1977), full of synchronicities around the numbers 17 and 23. I wanted to see the RSA system verified on my pocket calculator. I wasn't interested in secrecy, so I picked $17 \times 23 = 391$ as my modulus. Then the only message I wanted to send was, of course, the number 137. I picked 5 as the encoding power (since Wilson also mentions "The Law of Five" in *Cosmic Trigger*). Then I got the big surprise:

$$(137)^5 = 137 \bmod (17 \times 23).$$

In other words, 137 codes as itself these encoding parameters. In fact I could have chosen any odd number as the encoding power.

$$(137)^{\text{odd}} = 137 \bmod (17 \times 23).$$

And also: $(137)^{\text{even}} = 1 \bmod (17 \times 23).$

Could it be that the reason that we "see" 137 as the most fundamental pure number in physics (other than 1), is that 137 codes as itself according to the modulus 17×23 .

Yes, I know that the fine structure constant is really $1/137.03604$, or something close to that (we're not sure of that last digit). But, a little known fact is that there is strange Pythagorean relationship:

$$137^2 + (\pi)^2 = (137.03602\dots)^2$$

Also, of course, when we look at interactions at smaller and smaller distances, the electromagnetic coupling constant (which is what $1/137$ is really all about), becomes unified with the other force coupling constants. It is believed that the grand unified theory (GUT) coupling constant is $1/40$. The particle physicist Frank Close in *The Cosmic Onion* calls it $1/42$, and suggests it (tongue-in-cheek) as the *Hitchhiker's Guide to the Galaxy* (Douglas Adams) number. So the answer 42 is matched to the question, "what is the GUT number?"

Now this number 42 comes up in error-correcting code theory in the form of Gleason's theorem (which some regard as the most fundamental idea in coding theory. One should know that error-correcting codes are the opposite of cryptographic codes. An error-correcting code (such as a Hamming code) is used to keep information error free in a noisy environment; whereas, a cryptographic code is used to bury information in artificially constructed noise—very precisely constructed noise, of course. Thus there is a kind of duality between error-correcting codes and cryptographic codes. In fact the concept of Public Key Cryptography was invented by Marty Hellman as being dual to error-correcting codes. The RSA cryptography was invented as an early instantiation of Hellman's idea.

Given the strange RSA relationship between 137 and 17×23 , we need to check out the significance of these numbers in the context of error-correcting codes. Here it is useful to think of 17 and 23 as the code lengths of two error-correcting codes that are interweaved to make a bigger code of length 391. These two codes would be the Golay-23 code and the quadratic residue-17 code. The Golay code has 12 message carrying digits and 11 error correcting digits. The Quad-17 code has 9 message carrying digits, and 8 error correcting digits. Arranged in a rectangle, the 12×9 sector of 108 digits are message carrying. In order to avoid “burst errors” these codes would be interwoven via the “Chinese remainder theorem” (Cf. Berlecamp, *Algebraic Coding Theory*). One can do this by hand using a toroidal mapping on a 17×23 rectangle, and filling in the numbers 0 through 390 as follows:

000	069	138	207	276	345	023	092	161	230	299	368	046	115	184	253	322
323	001	070	139	208	277	346	024	093	162	231	300	369	047	116	185	254
255	324	002	071	140	209	278	347	025	094	163	232	301	370	048	117	186
187	256	325	003	072	141	210	279	348	026	095	164	233	302	371	049	118
119	188	257	326	004	073	142	211	280	349	027	096	165	234	303	372	050
051	120	189	258	327	005	074	143	212	281	350	028	097	166	235	304	373
374	052	121	190	259	328	006	075	144	213	282	351	029	098	167	236	305
306	375	053	122	191	260	329	007	076	145	214	283	352	030	099	168	237
238	307	376	054	123	192	261	330	008	077	146	215	284	353	031	100	169
170	239	308	377	055	124	193	262	331	009	078	147	216	285	354	032	101
102	171	240	309	378	056	125	194	263	332	010	079	148	217	286	355	033
034	103	172	241	310	379	057	126	195	264	333	011	080	149	218	287	356
357	035	104	173	242	311	380	058	127	196	265	334	012	081	150	219	288
289	358	036	105	174	243	312	381	059	128	197	266	335	013	082	151	220
221	290	359	037	106	175	244	313	382	060	129	198	267	336	014	083	152
153	222	291	360	038	107	176	245	314	383	061	130	199	268	337	015	084
085	154	223	292	361	039	108	177	246	315	384	062	131	200	269	338	016
017	086	155	224	293	362	040	109	178	247	316	385	063	132	201	270	339
340	018	087	156	225	294	363	041	110	179	248	317	386	064	133	202	271
272	341	019	088	157	226	295	364	042	111	180	249	318	387	065	134	203
204	273	342	020	089	158	227	296	365	043	112	181	250	319	388	066	135
136	205	274	343	021	090	159	228	297	366	044	113	182	251	320	389	067
068	137	206	275	344	022	091	160	229	298	367	045	114	183	252	321	390

If we disregard the first row and first column, we notice that the numbers 1, 254, 137, and 390 hold the corner positions of the 16×22 rectangle. These are the solutions to the equation:

$$137^{\text{odd}} = X \bmod(17 \times 23)$$

Note also that 254 is $391 - 137$, and that 390 is $391 - 1$, so that 137 is the basic solution X. In general one can solve such an equation via some toroidal mapping like that used here.