



Secrets of the HDX6144 Encryption Algorithm Paper 1: Multiple Fermat Sequence

Dr William McMullen Hawthorne

This Paper is written in the first person singular because it concerns events, many of which took place before Hawthorne Davies Ltd was formed.

A Multiple Fermat Sequence is a mathematical technique for generating a pseudo-random byte stream. Used in combination with another original concept - "Restricted Power Set" (RPS) prime number", it is fundamental to most of the research I have contributed to Hawthorne Davies' technology.

This paper introduces five concepts in a related logical order:

- 1 FERMAT SEQUENCE
- 2 GENERATOR
- 3 SEMI-GENERATOR
- 4 RESTRICTED POWER SET (RPS) PRIME
- 5 MULTIPLE FERMAT SEQUENCE (MFS)

The last three of these concepts are new and special to Hawthorne Davies' technology.

Fermat Sequence

In order to understand the MFS and RPS concepts, we first have to revive a theorem attributed to Pierre de Fermat (1601-65), which has applications in "Modular Arithmetic". A statement of the theorem is:

If M is a prime number
and A is an integer in the range 1 to $(M-1)$
and B is an integer in the range 1 to $(M-1)$
then $A \times B^{(M-1)} \text{ mod } M = A$

To give a simple numeric example, let us look at a set of sequences all formed by starting with a number "A" which is then successively multiplied by a number "B" and modulated by a prime number "M".

$M = 13$:

$A = 7$

	sequence														
B= 1	7	7	7	7	7	7	7	7	7	7	7	7	7	7	trivial
B= 2	7	1	2	4	8	3	6	12	11	9	5	10	7		
B= 3	7	8	11	7	8	11	7	8	11	7	8	11	7		
B= 4	7	2	8	6	11	5	7	2	8	6	11	5	7		
B= 5	7	9	6	4	7	9	6	4	7	9	6	4	7		
B= 6	7	3	5	4	11	1	6	10	8	9	2	12	7		
B= 7	7	10	5	9	11	12	6	3	8	4	2	1	7		
B= 8	7	4	6	9	7	4	6	9	7	4	6	9	7		
B= 9	7	11	8	7	11	8	7	11	8	7	11	8	7		
B=10	7	5	11	6	8	2	7	5	11	6	8	2	7		
B=11	7	12	2	9	8	10	6	1	11	4	5	3	7		
B=12	7	6	7	6	7	6	7	6	7	6	7	6	7	trivial	

Each sequence has a cyclic length. The cyclic lengths of $B = 1 \pmod{M}$ and $B = M-1 \pmod{M}$ are regarded as trivial.

Generator

This is not a new concept. The above table shows that $B = 2,6,7,11$ are "generators" because they generate a cycle, which includes all elements of the set: $\{1,2,3,4,5,6,7,8,9,10,11,12\}$. All four sequences have a cyclic length of 12.

Semi-generator

$B = 4, 10$ are semi-generators because they generate half of the complete set. Another way of looking at the above structure is to consider the idea of the "power" of the generator. So $B = 2,6,7,11$ have a power of 12, $B = 4, 10$ have a power of 6

The table of powers for $M = 13$ is:

B =	2	3	4	5	6	7	8	9	10	11
Power =	12	3	6	4	12	12	4	3	6	12

The power of B with respect to M is therefore equivalent to the cyclic length of B with respect to M .

Restricted Power Set Primes

The set of (non-trivial) Powers for $M = 13$ is $\{3,4,6,12\}$

For $M = 11$ the set of powers is $\{5,10\}$

For $M = 47$ the Set of powers is $\{23,46\}$

For $M = 59$ the set of powers is $\{29,58\}$

The name I have coined for prime numbers, for which all values in the range $1 < B < (M-1)$ are either generators or semi-generators, is "Restricted Power Set"(RPS) Primes. The constraint on P is that $(P-1)/2$ is also prime. It is interesting to note that all RPS primes belong to the remainder class 11 modulo 12. It should also be noted that if P is an RPS prime, the number of generators and semi-generators are each equal to $(P - 3) / 2$.

Modulator: 227

		generators										semi-generators									
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21		
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41		
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61		
62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81		
82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101		
102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121		
122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141		
142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161		
162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181		
182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201		
202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221		
222	223	224	225																		

G = 112 S = 112

Multiple Fermat Sequence

We will now construct a simple Multiple Fermat Sequence by adding two Fermat Sequences constructed from two semi-generators and modulated by two distinct primes, and further modulated by 10 after addition:

M = 47 A = 11 B = 16 (semi-generator)

M = 59 A = 34 B = 27 (semi generator)

```
8948825633820542746677389759665787488639999359841234650588970881725613
7481060422697359581910557022137802927233812819664713100144508198665576
6742729463633021399133611165297340424705723451447412410884274198179432
7953774664471157810657363029578769047338643953667336622518794539797131
0471665965963945701838430576196039666598953202626914228991039789803435
6183254914439738427723598973484062618537535830353534111035534558560836
1113958583580596791901932382843430279767280428772001646835373626542280
4341009501858515912823417210366427934332330767758157302272057417899409
6068098822679541050359319863190759371464241596802725499325839978275405
4072810341932170039073126772841412035
```

Cyclic length = 667

My earliest encryption algorithm, codenamed HMX, simulated a three-loop Vernam cipher. "Loop" is a term no longer used. The current jargon word is "wheels". Each wheel was a Fermat Sequence based on an RPS prime. HMX was shown to the Computer Electronic Security Group at GCHQ in 1984. I still have a record and a summary report on file. The scalability of the cipher was the subject of considerable interest and I demonstrated that a 20-wheel version with cyclic length 1.26×10^{84} and a potential key strength of 595 bits, could be created by altering one variable. This was a rather new idea in 1984.

The demonstration program was written in BASIC in 3 Kbytes of code. The same three wheel version was the subject of a detailed report by Professor Fred Piper, commissioned in December 1989. Professor Piper was, at that time, Professor of Mathematics at Royal Holloway College, ran a consultancy called Codes and Ciphers Ltd, and is joint author of a standard text on cryptology. The most significant paragraph in Professor Piper's report is:

"...one objective for the designer of a cryptographic algorithm is to ensure that an exhaustive key search offers the 'fastest' form of attack. One of the conclusions of this report is that the designers of the HMX Algorithm achieve this objective...."

HFX40 Cipher for Secure Facsimile is a development of the HMX Cipher and is now part of the International Telecommunication Union's Recommendation T.36. The original HMX Cipher is used, in hardware form, by the banking industry.

The MFS-3 stream in the HMX algorithm has a theoretical cyclic length of $16301 \times 16253 \times 32182 = 8,526,827,057,892$.

If we confine the stream to MFS-2, then we can apply the Accumulated Maximum Runs Test (ref: The Carousel Random Generator Paper 2):

If 16 is a semi-generator of 32603 and 27 is a semi-generator of 32507 then the theoretical cyclic length $= 16302 \times 16253 = 264,940,153$

The predicted cyclic length is confirmed by the AMR Test:

Limit: 24

3 4 5 6 7 910111213161920222324	46518912
1 2 8 911121314192028	7715525
1 3 6 7 8 9131517222327	27969533
3 4 5 6 7 9111213151718192021222326	95493380
2 6 7 8 914161718212225	15859871
1 2 3 5 6 81518192125	14880194
1 5 7 8 9141516202224	18259604
1 5 6 7 9101315182021222324	84762046
1 2 8 911121314192028	7715525

Cyclic length = 7715525
 27969533
 95493380
 15859871
 14880194
 18259604
 84762046

 264940153

Euclid proved, in what is probably the most elegant one-line proof in the whole of mathematics, that the set of prime numbers is infinite, by showing that, for any given prime, however large, there exists a prime that is greater:

If P is prime then consider: $L = (2.3.5.7.11 \dots P) + 1$

If L is prime it is greater than P, but if L is not prime then there exists a prime factor of L which is greater than P.

To exemplify Euclid's proof:

P = 11

$L = 2.3.5.7.11 + 1 = 2311$: 2311 is prime and greater than 11

P = 13

$L = 2.3.5.7.11.13+1 = 30031 = 59.509$: 59 is prime and greater than 13

Euclid's proof has set me wondering if there is a logical proof that the set of RPS primes is infinite. The first 100,000 RPS primes look like this;

Serial number	RPS prime	interval
1	11	11
2	23	12
3	47	24
4	59	12
99,998	38,782,727	384
99,999	38,783,483	756
100,000	38,783,939	456

This, of course, is not a proof, merely data which adds some plausibility to my conjecture. The mystery is further compounded by the seeming lack of pattern in the intervals between successive RPS primes, other than the obvious fact that all intervals except the first are multiples of 12.

On behalf of Hawthorne Davies Ltd, may I express my admiration in advance to any mathematician who succeeds in constructing a formal proof. We would very much like to read it.