Introduction to Cryptology

Lecture-07

Secret-Key Ciphers

Stream Ciphers: Design Principles

26.04.2023, v50

Stream Ciphers

Design Fundamentals

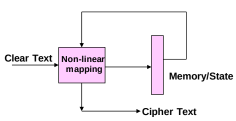
Outlines

- Historical Overview
- Basic Definitions
- Linear Feedback Shift Register Sequences
- Stream Cipher Design Principles
- Contemporary Standards

Stream Cipher Structures

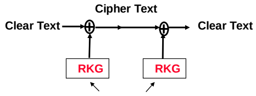
One particular property: The cipher includes an internal **memory**

General form
stream-ciphering-machine



Non-linear finite state machine

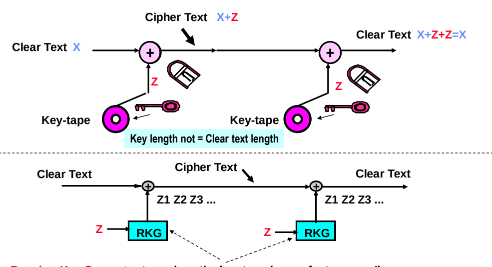
Most used special form
Additive stream ciphering-machine using Running-Key-Generator RKG



(Running Key Generator RKG)

(This lecture is limited to describe such stream ciphers as the most widely used stream cipher structures)

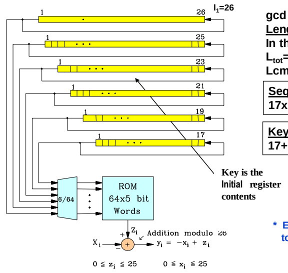
Additive Stream Cipher Similar to the perfect Vernam Ciphers 1926



Running Key Generator to replace the key-tape (no perfect secrecy!): Example: A5 in GSM

Stream Cipher Hagelin M-209 (2nd World War)

designed by the Swedish cryptographer Boris Hagelin in the 1930s *.



gcd $(l_i, l_j)=1$
Lengthes are relatively prime!
In that case total sequence length is:
$L_{tot} = \text{lcm}\ (l_1 \ldots l_t)$
Lcm: least common multiple

Sequence Length =
$17 \times 19 \times 21 \times 23 \times 25 \times 26 \approx 10^8$ bits

Key Length = total register size =
$17+19+21+23+25+26 \approx 131$ bits

* Electronic equivalent structure to the real mechanical machine

Most Modern Stream Ciphers are basically Key Stream Generators KSGs

Most Modern Stream Ciphers deploy the so called:
"Linear Feedback Shift Registers" LFSR
(linear state machines)
as building blocks for constructing Key Stream Generators (KSGs)

The design rules for LFSRs are therefore presented in a compact form in the next slides

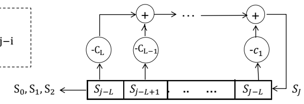
A good reference on this subject is:
Golomb, S.W.: Shift Register Sequences. Holden-Day, Inc., San Francisco (1967); Revised 2nd edn., Aegean Park Press, Laguna Hills, CA (1982)

Linear Feedback Shift Registers LFSR

Linear Sequence Generator (canonical form 1)
D-transform format (also known as Fibonacci LFSRs)

$$S_j = -\sum_{i=1}^{L} c_i S_{j-i}$$

for $j \geq L$



Register has length L

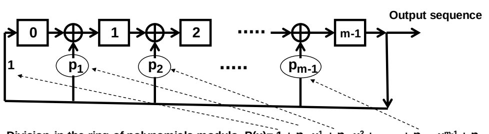
Feedback is defined by the Connection Polynomial in the delay element D:

$C(D) = 1 + C_1 D^1 + C_2 D^2 + ... + C_L D^L$

We restrict our treatment for binary case that is over GF(2)

Linear Feedback Shift Registers LFSR

Linear Sequence Generator (canonical form 2)
equivalent to form 1 (also known as Galois LFSRs)
Division engine in the ring of polynomials modulo p(x) $Z_{p(x)}$



Division in the ring of polynomials modulo $P(x)= 1 + p_1 x^1 + p_2 x^2 + ... + p_{m-1} x^{m-1} + p_m x^m$

Polynomial degree = m

Feedback Shift Register similarity to division in rational numbers

A rational number is represented by the division a/b, where a and b are coprime integers such that gcd (a,b)=1

Example: The division 1/7 = 0.142857 142857 142857..

Sequence with a Cycle-length = 6

LFSR output sequence is equivalent to dividing two polynomials: $S(D) = \frac{P(D)}{C(D)}$

Example: $S(D) = \frac{P(D)}{C(D)} = \frac{1+D}{1+D+D^2}$ (see Ref. Golomb. For D-transform division)

$S(D) = (1 + D) \div (1 + D + D^2) = 1 + D^2 + D^3 + D^5 + D^6 + D^8....$

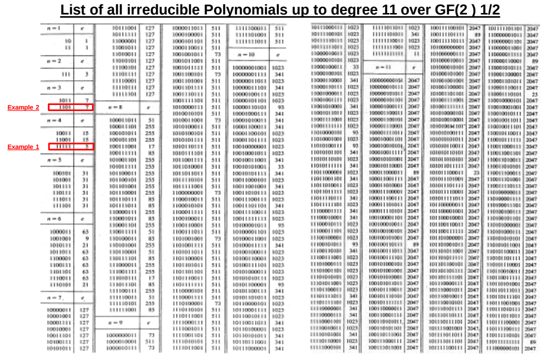
$1 + D + D^2$
D^2
$D^2 + D^3 + D^4$
$D^3 + D^4$
$D^3 + D^4 + D^5$
D^5
$D^5 + D^6 + D^7$
$D^6 + D^7$
$D^6 + D^7 + D^8$
D^8 ....

MSB .... LSB

101 101 101

Cycle length=3

List of all irreducible Polynomials up to degree 11 over GF(2) 1/2



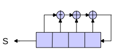
Basic Linear Feedback Shift Register Structure LFSR

Example 1 (using irreducible polynomial with period 5)

$C(D) = D^4 + D^3 + D^2 + D + 1=11111$

Is irreducible (non-primitive) with period N = e = 5, → Cycle-length of each loop = 5

N divides 2^4-1 = 15 (see list of irreducible polynomials)

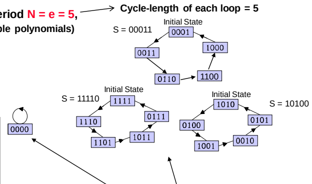


(See canonical form 1)

Period N=5 of irreducible polynomial of degree L divides $2^L-1 = 2^4-1 = 15$ its cycle structure is:

$$\left\{1(1), \frac{2^L-1}{N}(N)\right\}$$

Any irreducible polynomial creates a similar structure including such loops having equal periods = e.
e is a divisor of 2^L-1



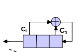
Cycle structure:{1(1), 3(5)}.

Reducible Polynominals do not create equal cycles !!!

LFSR Using a Primitive Polynomials

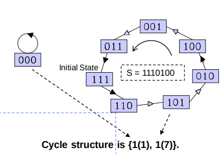
Example 2: - Primitive polynomial with maximum period
- Results with all non-zero elements in one loop
- Resulting with the so called Pseudo-Noise (PN)-Sequence

$C(D) = D^3 + D + 1 = 1011$
is irreducible and primitive with period $e = N = 2^3-1 = 7$.



Output sequence: 1 1 1 0 1 0 0

Window property



Cycle structure is {1(1), 1(7)}.

PN-Sequence properties for L=m=3:

1. The sequence length is $2^m-1 = 7$
2. The number of 1's is $2^{m-1} = 4$
3. The number of 0's is $2^{m-1}-1 = 3$
4. A shifted window of length m=3 on the sequence results with all $2^m-1 = 7$ non-zero m-bit binary patters (Window property)
5. The polynomial used and its reciprocal (mirrored pattern) result with the same sequence length $C^*(D) = D^3 C(D^{-1}) = D^3 + D^2 + 1$
6. The number of primitive polynomials of degree m over GF(2) is: $\varphi(2^m-1) / m = 2$

LFSR as PN-Sequence Generator

(maximum-Length Sequence)

(Pseudo-Noise) PN-Sequence Characteristics

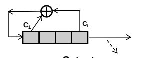
Generalization: If the connection or division Polynomial of degree m is selected to be a **primitive Polynomial**, that is an irreducible polynomial , where the order of x is $=2^m-1$ (the highest possible order/period), then the output sequence is called a **Pseudo-Noise** (PN) Sequence.

In general, PN Sequences have the following properties:

1. The sequence length is 2^m-1
2. The number of 1's is 2^{m-1}
3. The number of 0's is $2^{m-1}-1$
4. A shifted window of length m on the sequence results with all 2^m-1 non-zero m-bit binary patters (Window property)
5. If the reciprocal polynomial (mirrored pattern) is used, then it results with the same sequence length with mirrored sequence.
6. The number of primitive polynomials over GF(2) is: $\varphi(2^m-1)/m$

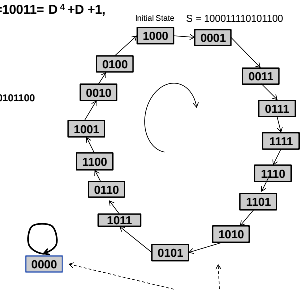
Example: LFSR , as PN Sequence generator of length $2^4 - 1 = 15$

If C(D) is a primitive polynomial $C(D) = 10011 = D^4 + D + 1$,
Then its periode $N = 2^4 - 1 = 15$.



Sequence properties for m=4:

1. The sequence length is $2^m-1= 15$
2. The number of 1's is $2^{m-1} = 8$
3. The number of 0's is $2^{m-1}-1 = 7$
4. A shifted window of length m=4 bits on the sequence results with all $2^m-1= 15$ non-zero 4-bit binary patters (window property)
5. The polynomial used and its reciprocal mirrored pattern result with the same sequence length $C^*(D)=D^4+D^3+1$
6. The number of primitive polynomials of degree m over GF(2) is :
$\varphi(2^m-1)/m = \varphi(2^4-1)/4 = 2$



Cycle structure is { 1(1) , 1(15) }

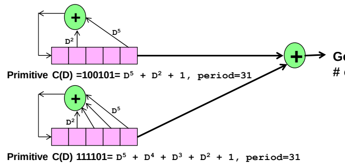
Applications of PN-Sequence Generator

Two examples

1. Radar Distance Measurement :
PN Sequence shift is proportional to the delay time of a reflected wave.

2. 3rd Generation Mobile multiple access CDMA system uses PN Sequences

Gold Sequences C_i s:
Are orthogonal Sequences generated by combining PN-Sequences with the cross-correlation property $C_i(t) \times C_j(t) \approx 0$ for $i \neq j$ to differentiate between users sending on the same broadband channel. Every user is assigned a different sequence. As in the following example:

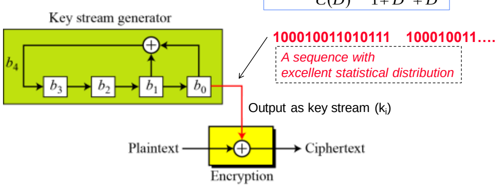


LFSR Linear Feedback Shift Register

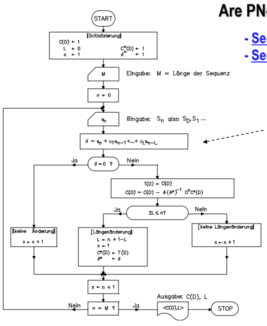
PN-sequence as a Running Key Generator?

Primitive polynomial $C(D) = D^4 + D^3 + 1$ of degree 4
=> period $N = 2^4-1 = 15$

$$S(D) = \frac{P(D)}{C(D)} = \frac{1+D}{1+D^3+D^4}$$



A bad Cipher ! Why?



Are PN-Sequences good for stream ciphers?

- Sequence randomness and quality: very good
- Security : very bad
due to Massey-Berlekamp Algorithm

Massey-Berlekamp Algorithm:
It is possible to find the shortest connection Polynomial C(D) and the initial value of the register if only 2L bits of the sequence are known

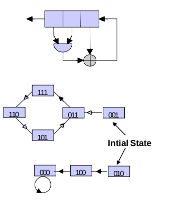
(**example**: sequence in the former page can be cracked if only 2x4=8 bits of the key stream are known)

Sequence Security quality is measured by:
The linear Complexity L(S) of a sequence **S** is: the length L in bits of the shortest LFSR that generates the sequence S.

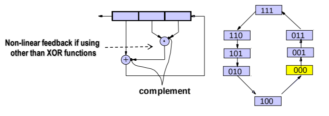
Non-Linear Feedback Shift Register Structure NLFSR

are good key-sequence generators: Singular and Non-singular cases

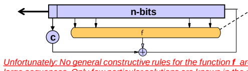
Non-linear Singular Shift Register Sequences



Non-linear Non-Singular Sequences



In General: The following n-bit register structure is Non-singular over GF(2) if $c \neq 0$
Where f : is any function (linear or non-linear)



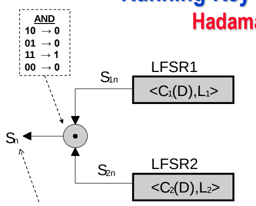
$\#|f| = 2^{2^{n-1}}$

For n=10
$\#|f| = 2^{512}$
Crypto-Significant!

*Unfortunately: No general constructive rules for the function **f** are known for large sequences. Only few particular solutions are known in the public literature!*

De-linearizing LFSR to use them as Running Key Generators (RKGs)

Hadamard Combiner



Bad output statistics of 1 and 0 distribution!
Reason: AND gate results with 75% of Zeros as output for all input combinations.

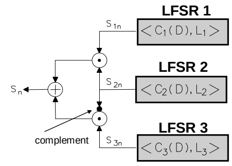
C_1(D) & C_2(D) irreducible with periods N_1, N_2 and degree L_1, L_2 such that $\gcd(L_1, L_2) = 1$

Linear complexity $L(S_0, S_1, S_2 ...) = L_1.L_2$
Sequence Period is $N = lcm(N_1, N_2) = N_1 . N_2$

$$N_1 = 2^{L_1} - 1,\ N_2 = 2^{L_2} - 1$$
$$Sequence\ length\ N = lcm(N_1, N_2) = lcm(2^{L_1} - 1, 2^{L_2} - 1)$$
$$N = \frac{(2^{L_1}-1)(2^{L_2}-1)}{\gcd(2^{L_1}-1, 2^{L_2}-1)} =$$
$$N = \frac{(2^{L_1}-1)(2^{L_2}-1)}{2^{\gcd(L_1,L_2)}-1} = (2^{L_1}-1)(2^{L_2}-1) = N_1 \bullet N_2$$

Running Key Generators

Geffe´s Running Key Generator



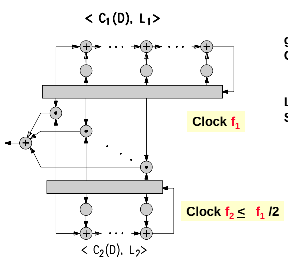
C_1(D), C_2(D) and C_3(D) irreducible with periods N_1, N_2 N_3 and degree L_1, L_2, L_3 such that $\gcd(L_i, L_j) = 1$

Linear complexity $L(S_n) = L_3 + L_1.L_2 + L_2.L_3$
Sequence Period is $N = lcm(N_1, N_2, N_3)$

Better distribution of 1's and 0's !

Running Key Generators

Massey-Rueppel (Proposal ESA Satellite Images)

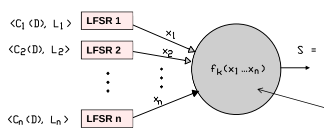


$\gcd(L_1, L_2) = 1$
C_1(D), C_2(D) are irreducible
$L_2 \leq L_1$

Linear complexity $L(S_n) = L_1.L_2$
Sequence Period is $N = lcm(N_1, N_2)$

Running Key Generators

Non-linear Combination of LFSR Sequences



Number of possible functions = 2^{2^n}

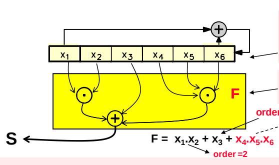
If $\gcd(L_i, L_j) = 1$ and C_1(D) ... C_n(D) are irreducible
then: $L(S_0, S_1,...S_n) = f_k(L_1, L_2,...L_n)$

Example: for $f_k(x_1, x_2, x_3) = x_1 + x_2x_3 + x_1x_2$ and $L_1 = 5$, $L_2 = 7$, $L_3 = 9$

$L(S_1, S_2, S_3) = L_1 + L_2L_3 + L_1L_2 = 5 + 7.9 + 5.7 = 103$

A Template for Designing a Running Key Generators

Non-linear Combination of LFSR Sequences



LFSR with primitive connection polynomial Of length L.
PN sequence: period $2^L-1 = 2^6-1=63$

Non-linear function F with non-linear order NLO=m

$F = x_1.x_2 + x_3 + x_4.x_5.x_6$

order =1
order =2
NLO= m= 3=L/2
Largest product of adjacent cells

$$\binom{L}{m} = \frac{L!}{m!(L-m)!}$$

If C (D) is primitive then the resulting linear complexity is: $L(\underline{S}) \geq \binom{L}{m} - (L-m)$

$$the\ function \binom{L}{m} = \frac{L!}{m!(L-m)!} \text{ has its peak at } m = L/2$$

$$L(\underline{S})_{Max} \rightarrow \binom{L}{L/2} > \frac{1}{L+1}2^L$$

For $m = L/2$
Linear Complexity $L(\underline{S}) \approx 2^{L-\log_2 L}$

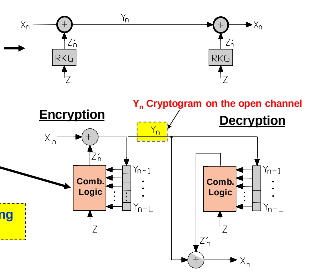
Design steps:

1. Select a primitive polynomial of degree L
2. Select a function F with a nonlinear order m=L/2
3. Select some low order terms in F (for good 1/0 distribution)
4. Compute effective linear complexity L(S)

Self Synchronizing Stream Cipher

Not Self Synchronising Cipher →

May be a Block Cipher
Or a highly non-linear function



Synchronises after communicating L subsequent error-free bits

Self Synchronising Cipher Without feedback!

The Most Widespread Stream Cipher

GSM Mobile Phone Cipher : A5/1,2 ..

Unpublished Ciphers !

Used in more than 7 000 million devices worldwide!

GSM: Mobile Phone A5/1 Stream-Cipher

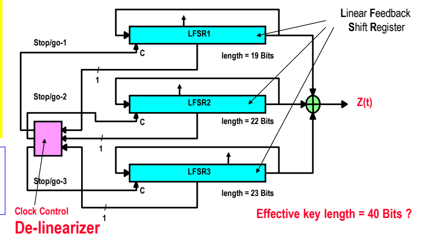
Secret Cipher!

Published by Berkely Students. (A standard Cipher cannot be kept secret !)

Effectively attacked by A. Shamir 1999/2000

The attack can find the key in less than a second on a single PC with 128 MB RAM and two 73 GB hard disks, by analysing the output of the A5/1 algorithm in the first two minutes of the conversation

It is unprofessional to assume that a cipher can be kept secret if somebody knows it !!

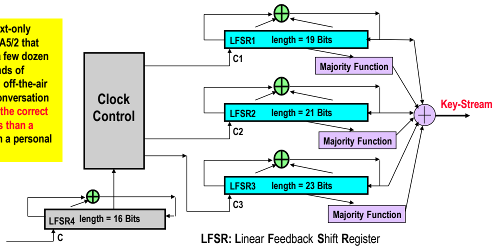


Effective key length = 40 Bits ?

The Reaction of GSM Association was: another secret Mobile Phone Cipher A5/2

Export version cracked by Barkan, Biham and Keller August. 2003

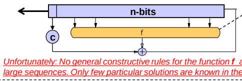
a ciphertext-only attack on A5/2 that requires a few dozen milliseconds of encrypted off-the-air cellular conversation and finds the correct key in less than a second on a personal computer



LFSR: Linear Feedback Shift Register

Sequences from Non-Linear Feedback Shift Register NLFSR (optional)

In General: The following n-bit register structure is Non-singular over GF(2) if $c \neq 0$
Where f : is any function (linear or non-linear)



$\#|f| = 2^{2^{n-1}}$

For n=10
$\#|f| = 2^{512}$
Crypto-Significant!

*Unfortunately: No general constructive rules for the function **f** are known for large sequences. Only few particular solutions are known in the public literature!*

Bounds

Largest possible sequence length from a state machine of n-bits:

when a machine starts by any initial state out of all 2^n possible states.

Upper bounds:

The autonomous state machine produces a sequence of length of at most: 2^n bits

There exist : 2^{2^n} possible sequences having the length 2^n

Which sequences have optimized equal distribution of 1's and 0's ?

De Bruijn Sequences

What is a De Bruijn Sequence?

Example for 8-bit De Bruijn Sequence of length 2^3=8 :

0-0-0-1-0-1-1-1-0-0-0

Sequential Window Values left to right: 0 1 2 5 3 7 6 4 0,1,2 …

Significant crypto-properties:

- Good statistical distribution of 1s and 0s as key sequences

- Large number of sequences compared with the linear PN sequences

Facts around the De Bruijn Sequences

- The binary **De Bruijn sequences:** Are binary sequences having the period of $P=2^n$ such that every n-bit tuple appears just one time in the sequence.
- the number of cyclically equivalent De Bruijn sequences B_n:

$$B_n = 2^{2^{n-1}-n}$$

– the weight of the sequence is 2^{n-1} that is 50% zeros and 50% ones

– Large linear complexities C : $2^{n-1} + n \leq C \leq 2^n - 1$

Example: for $n=3$

Sequence period: 2^3=**8** bits Sequence weight: 2^{3-1} =**4**

Num of sequences: $B_n = 2^{2^{n-1}-n} = 2^{2^{3-1}-3} = 2^{4-3} =$ **2**

For each sequence there is a reverse sequence in the sequence set

The 2 sequences are: 0 0 0 1 0 1 1 1 (0 1 2 5 3 7) 1 1 1 0 1 0 0 0 (7 3 5 2 1 0)

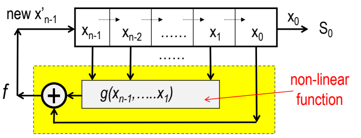
Mirror sequence

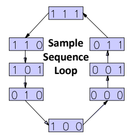
Reverse sequence

General Non-singular Fibunacci NLFSR

Proposed NLFSR Logic Structures: for De Bruijn Sequences Generators

The NLFSR is non-sigular if and only if: $f(x_0, x_1, \ldots, x_{n-1}) = x'_{n-1} = x_0 + g(x_1, \ldots, x_{n-1})$





non-singular = states in distinct loops

i.e.: If every generated output sequence is periodic for all probable initial states.

Two types of De Bruijn Sequences

1. **De Bruijn sequences of full length=2^n**
   - Are sequences of period $P=2^n$.
   - Where (n) is the length of the FSR
   - Total number of sequences: $B_n = 2^{2^{n-1}-n}$
2. **Modified De Bruijn sequences of length 2^n-1**
   - Are sequences of period $P=2^n-1$.
   - Total number of sequences: $B_n = 2^{2^{n-1}-n+1}$

Properties:

- good randomness properties, large classes and large linear complexities C :

$$2^{n-1} + n \le C \le 2^n - 1$$

Cryptographic Significance of De Bruijn Sequences

For n=2:

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n - 1 = 3}) = 2^{2^{n-1}-n+1} = 2^{2^{2-1}-2+1} = \mathbf{2}$

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n = 4}) = 2^{2^{n-1}-n} = 2^{2^{2-1}-2} = \mathbf{1}$

For n=3:

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n - 1 = 7}) = 2^{2^{n-1}-n+1} = 2^{2^{3-1}-3+1} = \mathbf{4}$

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n} = 8) = 2^{2^{n-1}-n} = 2^{2^{3-1}-3} = \mathbf{2}$

For n=4:

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n} - \mathbf{1} = \mathbf{15}) = 2^{2^{n-1}-n+1} = 2^{2^{4-1}-4+1} = \mathbf{32}$

$Total\ number\ of\ \mathbf{sequences}\ of\ Period\ (\mathbf{P = 2^n = 16}) = 2^{2^{n-1}-n} = 2^{2^{4-1}-4} = \mathbf{\mathit{16}}$

For n=5:

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n - 1 = 31}) = 2^{2^{n-1}-n+1} = 2^{2^{5-1}-5+1} = \mathbf{4096}$

$Total\ \mathbf{number\ of\ sequences}\ of\ Period\ (\mathbf{P = 2^n = 32}) = 2^{2^{n-1}-n} = 2^{2^{5-1}-5} = \mathbf{2048}$

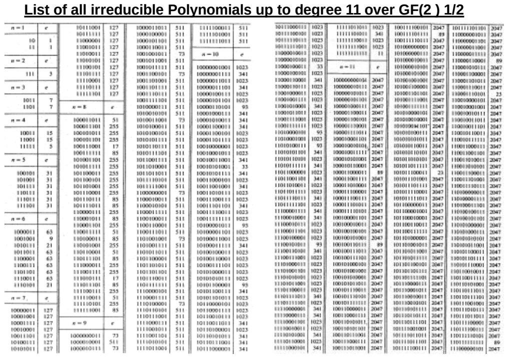
Sequences for larger n: implementation with adequate complexity is still unknown!!

- For **n = 6** there are $B_n = 2^{26}$ Sequences of length $2^n = 2^6 =$ **64** Bits
- For **n = 7** there are $B_n = 2^{57}$ Sequences of length $2^n = 2^7 =$ **128** Bits
- For **n = 8** there are $B_n = 2^{121}$ Sequences of length $2^n = 2^8 =$ **256** Bits
- For **n = 12** there are $B_n = 2^{2041}$ Sequences of length $2^n = 2^{12} =$ **4096** Bit

Annex

- **Full list of irreducible Polynomials up to degree 11**
- **List of all Primitive Polynomials up to degree 11**
- **Few Trinomials of higher degrees**
- **Factorizing 2^n-1 for n= 1 to 34**

List of all irreducible Polynomials up to degree 11 over GF(2) 1/2



List of all irreducible Polynomials up to degree 11 over GF(2) 2/2

111000011101	2047	111001111011	2047	111011111001	2047	111110010001	2047
111000100001	2047	111001111101	2047	111100001011	2047	111110010111	2047
111000100111	2047	111010000001	2047	111100011001	2047	111110011011	2047
111000101011	2047	111010010011	2047	111100110001	2047	111110100111	2047
111000110011	2047	111010011111	2047	111100110111	2047	111110101101	2047
111000111001	2047	111010100011	2047	111101011101	2047	111110110101	2047
111001000111	2047	111010111011	2047	111101101011	2047	111111001101	2047
111001001011	2047	111011001001	89	111101101101	2047	111111010011	2047
111001010101	2047	111011001111	2047	111101110101	2047	111111100101	2047
111001011111	2047	111011011101	2047	111101111001	89	111111101001	2047
111001110001	2047	111011110011	2047	111110000011	2047	111111111011	89

All Primitive Polynomials up to degree 11

2
111

3
1011
1101

4
10011
11001

5
100101
101001
101111
110111
111011
111101

6
1000011
1011011
1100001
1100111
1101101
1110011

7
10000011
10001001
10001111
10010001
10011101
10100111
10101011
10111001
10111111
11000001
11001011
11010011
11010101
11100101
11101111
11110001
11110111
11111101

8
100011101
100101011
100101101
101001101
101011111
101100011
101100101
101101001
101110001
110000111
110001101
110101001
111000011
111001111
111100111
111110101

9
1000010001
1000011011
1000100001
1000101101
1000110011
1001011001
1001011111
1001101001
1001101111
1001110111
1001111101
1010000111
1010010101
1010100011
1010100101
1010101111
1010110111
1010111101
1011001111
1011010001
1011011011
1011110101
1011111001
1100010011
1100010101
1100011111
1100100011
1100110001
1100111011
1101001111
1101011011
1101100001
1101101011
1101101101
1101110011
1101111111
1110000101
1110001111
1110110101
1110111001
1111000111
1111001011
1111001101
1111010101
1111011001
1111100011
1111101001
1111111011

10
10000001001
10000011011
10000100111
10000101101
10001100101
10001101111
10010000001
10010001011
10011000101
10011010111
10011100111
10011110011
10011111111
10100001101
10100011001
10100100011
10100110001
10100111101
10101000011
10101010111
10101101011
10110000101
10110001111
10110010111
10110100001
10111000111
10111100101
10111110111
10111111011
11000010011
11000010101
11000100101
11000110111
11001000011
11001001111
11001011011
11001111001
11001111111
11010001001
11010110101
11011000001
11011010011
11011011111
11011111101
11100010111
11100011101
11100100001
11100111001
11101000111
11101001101
11101010101
11101011001
11101100011
11101111101
11110001101
11110010011
11110110001
11111011011
11111110011
11111111001

11
100000000101
100000010111
100000101011
100000101101
100001000111
100001100011
100001100101
100001110001
100001111011
100010001101
100010010101
100010011111
100010101001
100010110001
100011001111
100011010001
100011100001
100011100111
100011101011
100011110101
100100001101
100100010011
100100100101
100100101001
100100111011
100100111101
100101000101
100101001001
100101010001
100101011011
100101110011
100101110101
100101111111
100110000011
100110001111
100110101011
100110101101
100110111001
100111000111
100111011001
100111100101
100111110111
101000000001
101000000111
101000010011
101000010101
101000101001
101001001001
101001100001
101001101101
101001111001
101001111111
101010000101
101010010001
101010011101
101010100111
101010101011
101010110011
101010110101

The number of primitive polynomials of degree *m* over GF(*2*) is: $\varphi(2^m - 1) / m$

Larger Primitive Polynomials

22
11000000000000000000001
10000000000000000000011

23
100001000000000000000001
100000000100000000000001
100000000000001000000001
100000000000000000100001

24
1000000000000000010000111
1110000100000000000000001

25
10010000000000000000000001
10000001000000000000000001
10000000000000000010000001
10000000000000000000001001

26
100000000000000000001000111
111000100000000000000000001

27
1000000000000000000000010111
1110100000000000000000000001

28
10000000000000000000000001001
10010000000000000000000000001

29
100000000000000000000000000101
101000000000000000000000000001

30
1000000100000000000000000000111
1110000000000000000000010000001

31
10000000000000000000000000001001
10010000000000000000000000000001

32
100000000010000000000000000000111
111000000000000000000100000000001

Factorization of 2^n-1

$2^3 - 1 = 7$
$2^4 - 1 = 3 \times 5$
$2^5 - 1 = 31$
$2^6 - 1 = 3 \times 3 \times 7$
$2^7 - 1 = 127$
$2^8 - 1 = 3 \times 5 \times 17$
$2^9 - 1 = 7 \times 73$
$2^{10} - 1 = 3 \times 11 \times 31$
$2^{11} - 1 = 23 \times 89$
$2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13$
$2^{13} - 1 = 8191$
$2^{14} - 1 = 3 \times 43 \times 127$
$2^{15} - 1 = 7 \times 31 \times 151$
$2^{16} - 1 = 3 \times 5 \times 17 \times 257$
$2^{17} - 1 = 131071$
$2^{18} - 1 = 3 \times 3 \times 3 \times 7 \times 19 \times 73$
$2^{19} - 1 = 524287$
$2^{20} - 1 = 3 \times 5 \times 5 \times 11 \times 31 \times 41$
$2^{21} - 1 = 7 \times 7 \times 127 \times 337$
$2^{22} - 1 = 3 \times 23 \times 89 \times 683$
$2^{23} - 1 = 47 \times 178481$
$2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$
$2^{25} - 1 = 31 \times 601 \times 1801$
$2^{26} - 1 = 3 \times 2731 \times 8191$
$2^{27} - 1 = 7 \times 73 \times 262657$
$2^{28} - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$
$2^{29} - 1 = 233 \times 1103 \times 2089$
$2^{30} - 1 = 3 \times 3 \times 7 \times 11 \times 31 \times 151 \times 331$
$2^{31} - 1 = 2147483647$
$2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537$
$2^{33} - 1 = 7 \times 23 \times 89 \times 599479$
$2^{34} - 1 = 3 \times 43691 \times 131071$