A5/1

Introducción

En las comunicaciones GSM se usan diferentes sistemas criptográficos dependiendo de la dimensión de la información a proteger: la identificación del usuario, su autenticación (A3), y la transmisión de datos y voz de forma cifrada (A5). Estos algoritmos están distribuidos entre el operador de la red GSM, el teléfono móvil y la propia SIM.

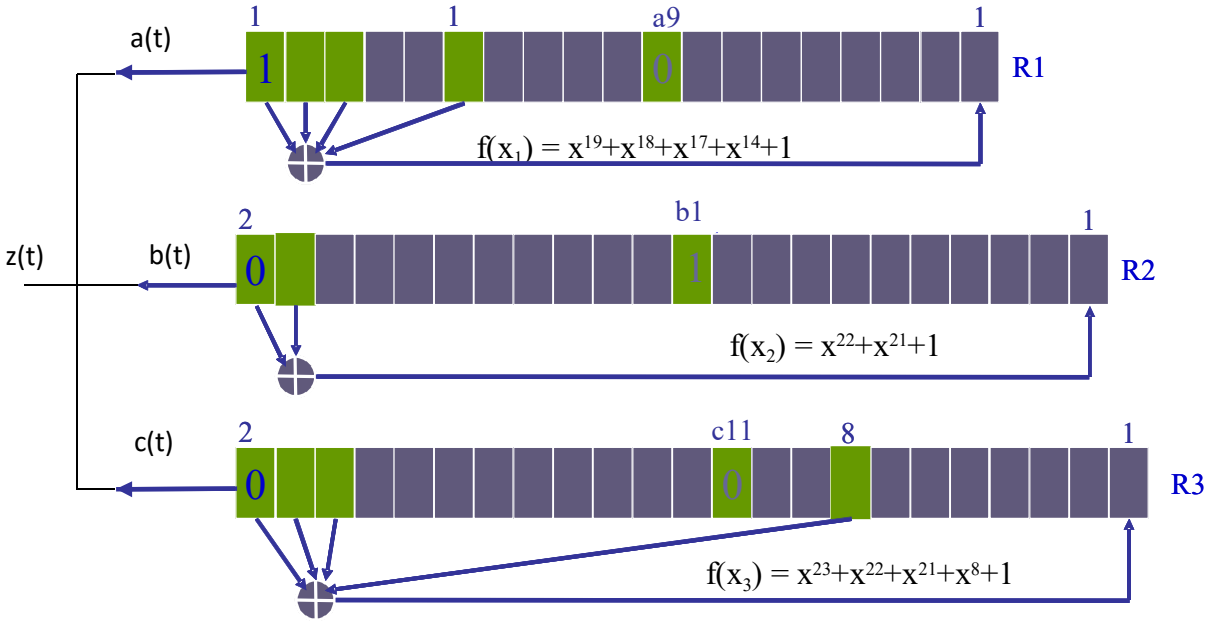
Existen tres variantes del A5, denominados A5/1, A5/2 y A5/3. El A5/1 se obtuvo por ingeniería inversa. Oficialmente, utiliza claves de 64 bits y el número de la trama de longitud 22 bits que es públicamente conocido. En 2008 se consigue criptoanalizar este cifrado disponiendo sólo de texto cifrado Barkan, Elad and Biham, Eli and Keller, Nathan", Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Advances in Cryptology - CRYPTO 2003”

Modificación: Inicialización oficial

1. **Cada uno de los tres registros de desplazamiento se inicializan con el estado cero. Los bits de salida no se utilizan y la función mayoría no se computa, está deshabilitada.**
2. **Los bits de la clave (semilla) se mezclan de acuerdo al siguiente proceso durante 64 ciclos. En un ciclo 0 <= i < 64, al bit que se calcula en cada registro como bit de realimentación para ser colocado en la posición menos significativa se le aplica un XOR con el i-ésimo bit de la clave: a[0] = a[0] ⊕ K[i], b[0] = b[0] ⊕ K[i], c[0] = c[0] ⊕ K[i]. El registro coloca el nuevo bit de realimentación y desplaza el contenido del registro.**
3. Posteriormente se procede de la misma manera calculando el bit de realimentación de cada polinomio con un XOR del bit correspondiente del número de trama o secuencia a cifrar. Esto se repite con cada uno de los 22 bits del número de trama. El registro coloca el nuevo bit de realimentación y desplaza el contenido del registro
4. Se habilita la función mayoría y se desplazan los registros durante 100 ciclos de acuerdo con los resultados de la función mayoría, descartándose los bits de salida.
5. Después de terminar esto, el algoritmo está listo para producir 2 secuencias de 114 bits de clave de flujo, una para cada dirección de la comunicación.

   Animación: https://www.youtube.com/watch?v=LgZAI3DdUA4

El cifrado A5 sigue el esquema siguiente:



Los polinomios utilizados son:

LFSR1: $p_1(x) = x^{19} + x^{18} + x^{17} + x^{14} + 1$, genera a(t)

LFSR2: $p_2(x) = x^{22} + x^{21} + 1$, genera b(t)

LFSR2: $p_3(x) = x^{23} + x^{22} + x^{21} + x^8 + 1$, genera c(t)

Además las posiciones que determinan la entrada a la función mayoría son: del LFSR1, la posición 9, del LFSR2, la posición 11 y por último, del LFSR3 la posición 11.

Dicha función mayoría viene definida por la expresión $F(a_9, b_{11}, c_{11}) = a_9 * b_{11} \oplus a_9 * c_{11} \oplus b_{11} * c_{11}$.

De esta forma, si el bit de la celda del registro coincide con el resultado de F, dicho registro estará en movimiento y se desplazará, en caso contrario no desplazará.

Un ejemplo de cómo se utiliza la función mayoría es el siguiente:

Supongamos $(a_9,b_{11},c_{11}) = (0,0,1)$ en la etapa i, entonces $F(a_9,b_{11},c_{11}) = 0$ con lo que los registros de desplazamiento 1 y 2 generarán en la siguiente etapa un nuevo bit cada uno y actualizarán sus estados, mientras que el LFSR3 mantendrá sin cambios su estado, generando en la etapa siguiente el mismo bit de salida.

Finalmente, la secuencia de salida del A5 se obtiene de la siguiente manera: $z(t) = a(t) \oplus b(t) \oplus c(t)$

A continuación se muestra una traza de los pasos 1 y 2 de la etapa de inicialización, ésta es la modificación que debes realizar en la práctica:

Semilla: K[i] dada como entrada

19	**18**	**17**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	0	0	1	0	0	0	1	0	0	0	1	1	0	1	0	0	0	1

41	**40**	**39**	**38**	**37**	**36**	**35**	**34**	**33**	**32**	**31**	**30**	**29**	**28**	**27**	**26**	**25**	**24**	**23**	**22**	**21**	**20**
0	1	0	1	1	0	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0

64	**63**	**62**	**61**	**60**	**59**	**58**	**57**	**56**	**55**	**54**	**53**	**52**	**51**	**50**	**49**	**48**	**47**	**46**	**45**	**44**	**43**	**42**
1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	0	0	1	1	1	1

Inicialización:

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Ciclo 1: a[1] = a[1] ⊕ K[1] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1

b[1] = b[1] ⊕ K[1] = 0 ⊕0 ⊕ 1 = 1

c[1] = c[1] ⊕ K[1] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Ciclo 2: a[1] = a[1] ⊕ K[2] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

b[1] = b[1] ⊕ K[2] = 0 ⊕ 0 ⊕ 0 = 0

c[1] = c[1] ⊕ K[2] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Ciclo 3: a[1] = a[1] ⊕ K[3] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

b[1] = b[1] ⊕ K[3] = 0 ⊕ 0 ⊕ 0 = 0

c[1] = c[1] ⊕ K[3] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Ciclo 4: a[1] = a[1] ⊕ K[4] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

b[1] = b[1] ⊕ K[4] = 0 ⊕ 0 ⊕ 0 = 0

c[1] = c[1] ⊕ K[4] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0

Ciclo 5: a[1] = a[1] ⊕ K[5] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

b[1] = b[1] ⊕ K[5] = 0 ⊕ 0 ⊕ 1 = 1

c[1] = c[1] ⊕ K[5] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1

Ciclo 6: a[1] = a[1] ⊕ K[6] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

b[1] = b[1] ⊕ K[6] = 0 ⊕ 0 ⊕ 0 = 0

c[1] = c[1] ⊕ K[6] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0

Ciclo 7: a[1] = a[1] ⊕ K[7] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

b[1] = b[1] ⊕ K[7] = 0 ⊕ 0 ⊕ 1 = 1

c[1] = c[1] ⊕ K[7] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1

Ciclo 8: a[1] = a[1] ⊕ K[8] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

b[1] = b[1] ⊕ K[8] = 0 ⊕ 0 ⊕ 1 = 1

c[1] = c[1] ⊕ K[8] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1
b		0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1

Ciclo 9: a[1] = a[1] ⊕ K[9] = 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0

b[1] = b[1] ⊕ K[9] = 0 ⊕ 0 ⊕ 0 = 0

c[1] = c[1] ⊕ K[9] = 0 ⊕ 0 ⊕ 0 ⊕ 1 ⊕ 0 = 1

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
b		0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
c	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1

Ciclo 10: $a[1] = a[1] \oplus K[10] = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 = 0$

$b[1] = b[1] \oplus K[10] = 0 \oplus 0 \oplus 0 = 0$

$c[1] = c[1] \oplus K[10] = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 = 0$

	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
a					0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0	0
b	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0	0	0
c	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1	0