

Proyecto # 1

1. MATERIALES

- Tarjeta **Raspberry Pi 3 Modelo B+**
- Micro SD y el adaptador de la Micro SD para el PC (Para guardar el OS)
- Cable micro USB para alimentar la tarjeta con “marranito”
- Cable de red (Opcional para conectar a un switch)
- DS18B20 – Sensor de temperatura

2. EJERCICIO

El propósito del proyecto es medir la temperatura ambiente, encriptar los datos y enviarlos a través de MQTT. Para encriptar los datos vamos a usar la técnica Simon.

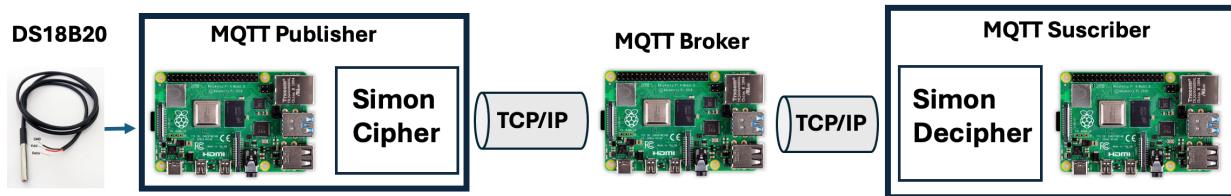


Figura 1. Descripción visual del proyecto # 1

La metodología es:

1. **Fase 1:** Leer la temperatura del sensor DS18B20 en la raspberry pi.
2. **Fase 2:** Cifrar los datos de temperatura usando la técnica de cifrado Simon.
3. **Fase 3:** Enviar los datos por MQTT.
4. **Fase 4:** Recibir los datos en el suscriptor MQTT.
5. **Fase 5:** Descifrar los datos en el suscriptor MQTT.

3. EVALUACIÓN

En la **semana # 6** de clases se debe entregar:

- **(Valor = 1.0)** Código comentado de la fase 1 y demostración en clase del funcionamiento
- **(Valor = 1.0)** Código comentado de la fase 2 y demostración en clase del funcionamiento
- **(Valor = 1.0)** Código comentado de la fase 3 y demostración en clase del funcionamiento
- **(Valor = 1.0)** Código comentado de la fase 4 y demostración en clase del funcionamiento
- **(Valor = 1.0)** Código comentado de la fase 5 y demostración en clase del funcionamiento

Por cada semana de retraso existe una penalización en la nota; por cada semana se descuenta una unidad (1.0).

El proyecto se hace en grupos de 3. Por cada miembro *adicional* del grupo se penaliza y descuenta media unidad (0,5) en la nota. Por ejemplo, para un grupo de 4 (Un miembro adicional) se califica sobre 4,5; para un grupo de 5 (Dos miembros adicionales) se califica sobre 4,0; etc.

ANEXO – CIFRADO Y DECIFRADO SIMON

Cifrado Simon: Para cifrar texto plano.

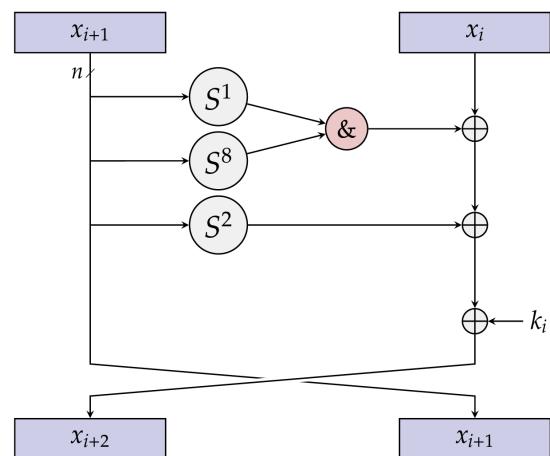


Figure 3.1: Feistel stepping of the SIMON round function.

Llave Simon: Para generar la llave en cada iteración.

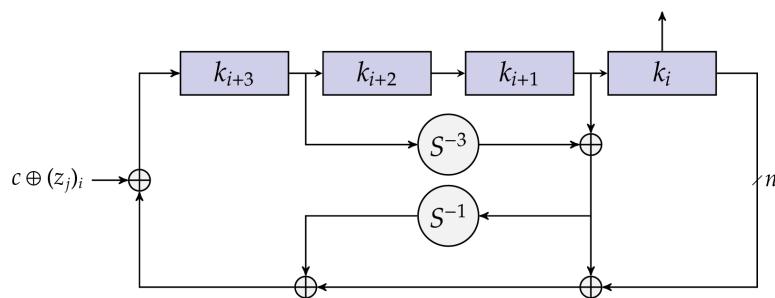
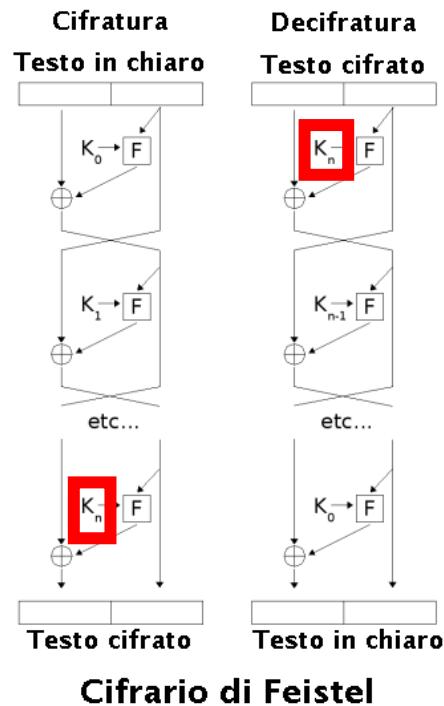


Figure 3.2: The SIMON two, three, and four-word key expansions.

Decifrado Simon: Simon es una red de Feistel y comparte sus propiedades.

- Las redes de Feistel presentan la ventaja de ser reversibles por lo que las operaciones de cifrado y descifrado son idénticas, requiriendo únicamente invertir el orden de las subclaves utilizadas.



EJEMPLO SIMON: Ejemplo para verificar que los valores que arroje la implementación son correctos.

Simon Example

Round #	Sub-Key	Lo	Ro	L ₁	R ₁
0	cdef	ooff	ooff	cfec	ooff
1	89ab	cfec	ooff	3a2e	cfec
2	4567	3a2e	cfec	462b	3a2e
3	123	462b	3a2e	2be6	462b
4	2f5a	2be6	462b	800	2be6
5	769c	800	2be6	5f7c	800
6	7292	5f7c	800	b3da	5f7c
7	af52	b3da	5f7c	7df5	b3da
8	e26a	7df5	b3da	570d	7df5
9	30d0	570d	7df5	1d02	570d
10	7083	1d02	570d	5182	1d02
11	9ae9	5182	1d02	4300	5182
12	9fdd	4300	5182	4396	4300
13	6de8	4396	4300	a653	4396
14	5380	a653	4396	c9fe	a653
15	3a6e	c9fe	a653	290f	c9fe
16	1fd6	290f	c9fe	701c	290f
17	4a52	701c	290f	a31c	701c
18	e6ca	a31c	701c	1E85	a31c
19	271b	1E85	a31c	fb19	1E85
20	59c3	fb19	1E85	bb12	fb19
21	7ea4	bb12	fb19	7bd6	bb12
22	659f	7bd6	bb12	e7fc	7bd6
23	372f	e7fc	7bd6	43497	e7fc
24	f25e	43497	e7fc	4118	43497
25	6766	4118	43497	7cec	4118
26	9c41	7cec	4118	c6bo	7cec
27	6gef	c6bo	7cec	8f80	c6bo
28	42d5	8f80	c6bo	ba66	8f80
29	368d	ba66	8f80	341f	ba66
30	cb1c	341f	ba66	a932	341f
31	207e	a932	341f	a28a	a932

REFERENCIAS

- Simon chiper https://youtu.be/gW87_TTaf2A?feature=shared
- Ray, B., Douglas, S., Jason, S., Stefan, T. C., Bryan, W., & Louis, W. (2013). *The simon and speck families of lightweight block ciphers*. Technical report, Cryptology ePrint Archive, Report./404. <https://eprint.iacr.org/2013/404.pdf>