

Universidade Federal de Santa Maria - UFSM  
Centro de Tecnologia - CT  
Curso de Engenharia de Computação  
ELC1144 - Segurança de Rede

# *Radio-Frequency Identification (RFID)*

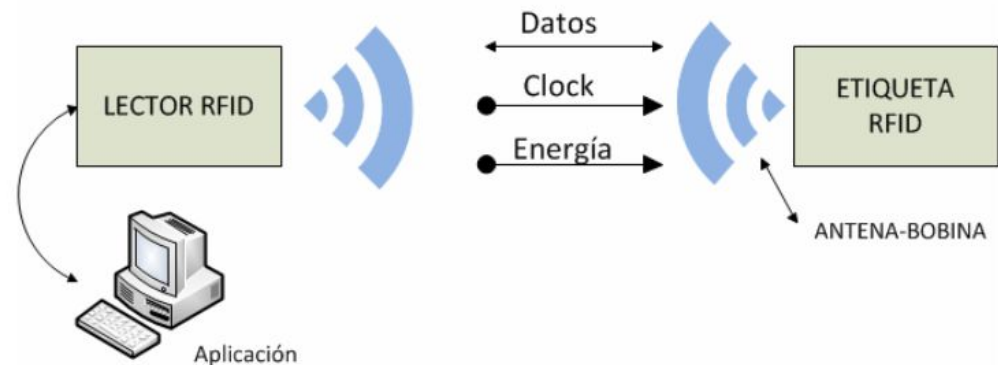


Luis Felipe de Deus - dedeus.f.l@gmail.com.

Dezembro/2019

# Introdução

- Comunicação usando ondas eletromagnéticas;
- Dados armazenados em uma etiqueta ou tag;
- Composto por:
  - Antena;
  - Transceptor;
  - Leitor;
  - Transponder.



# Tags

- Passivas:
  - Mais simples;
  - Não possui bateria;
  - Curtas distâncias;
- Ativas:
  - Fonte de energia própria;
  - Pode iniciar a comunicação;
  - Memória geralmente maior;
  - Custo e tamanho elevados.



# Vantagens

- Confiabilidade;
- Facilidade de leitura;
- Capacidade de armazenamento de dados;
- Otimização de processos;



# Desvantagens

- Interferência por metais;
- Custo elevado se comparado a código de barras;
- Distância de leitura;
- Segurança.



# Ameaças à Segurança

Suscetível a muitos tipos de ataques:

- *Sniffing*;
- *Tracking*;
- *Spoofing*;
- DOS (*Denial of Services*);
- MITM (*Man in the Middle*);



# Implementações de Segurança

- Criptografia;
- Chaves de acesso;
- Blindagem eletromagnética;
- Modulação.



# RFID Chips Mifare

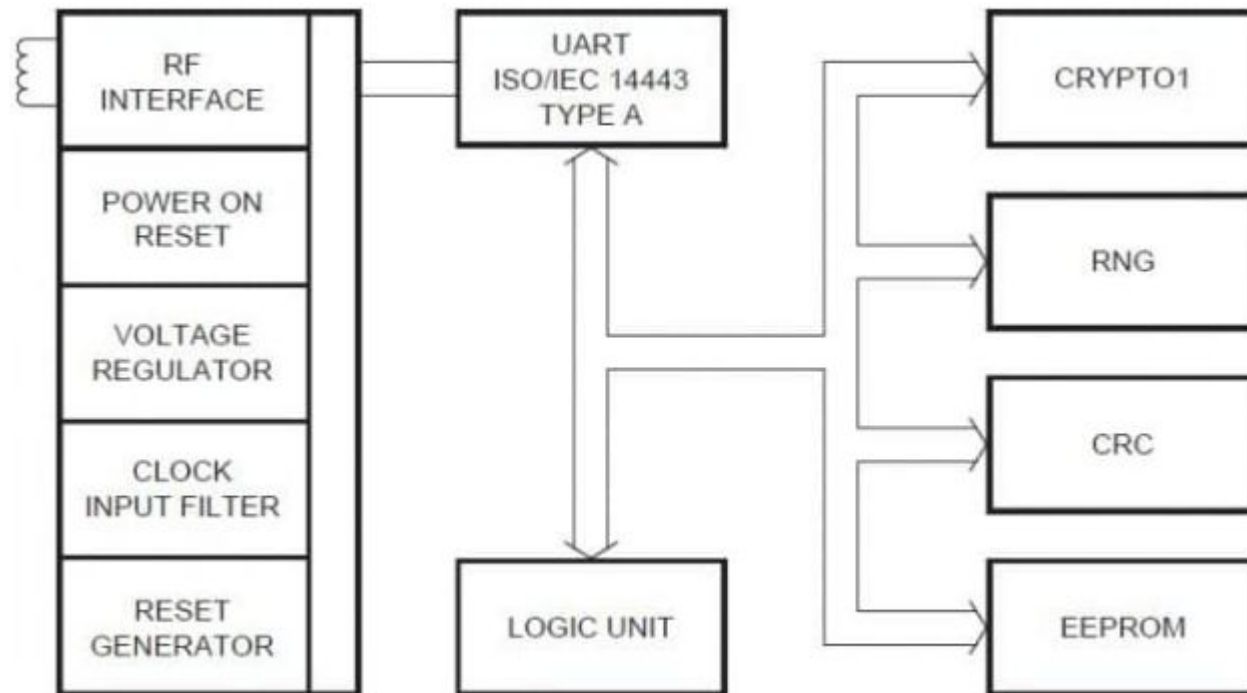
- Utiliza a banda de 13.56 MHz;;
- Divisão de blocos:
  - Bloco RF;
  - Anticolisão;
  - Unidade Lógica;
  - Unidade de Criptografia;
  - EEPROM.





# RFID Chips Mifare

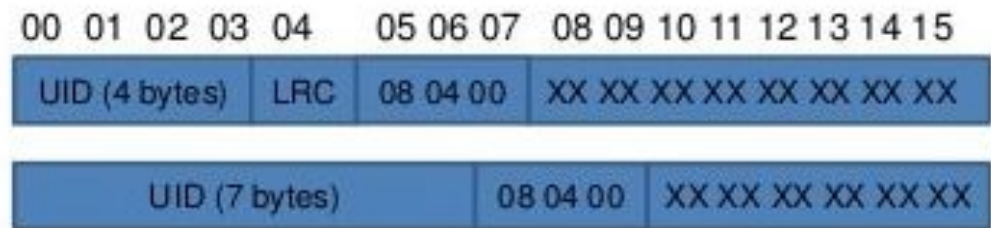
- Diagrama de Blocos:



# RFID Chips Mifare

## Estrutura de Memória:

- Divididos em setores;
- Setores divididos em blocos;
- Cada bloco possui 16 bytes.



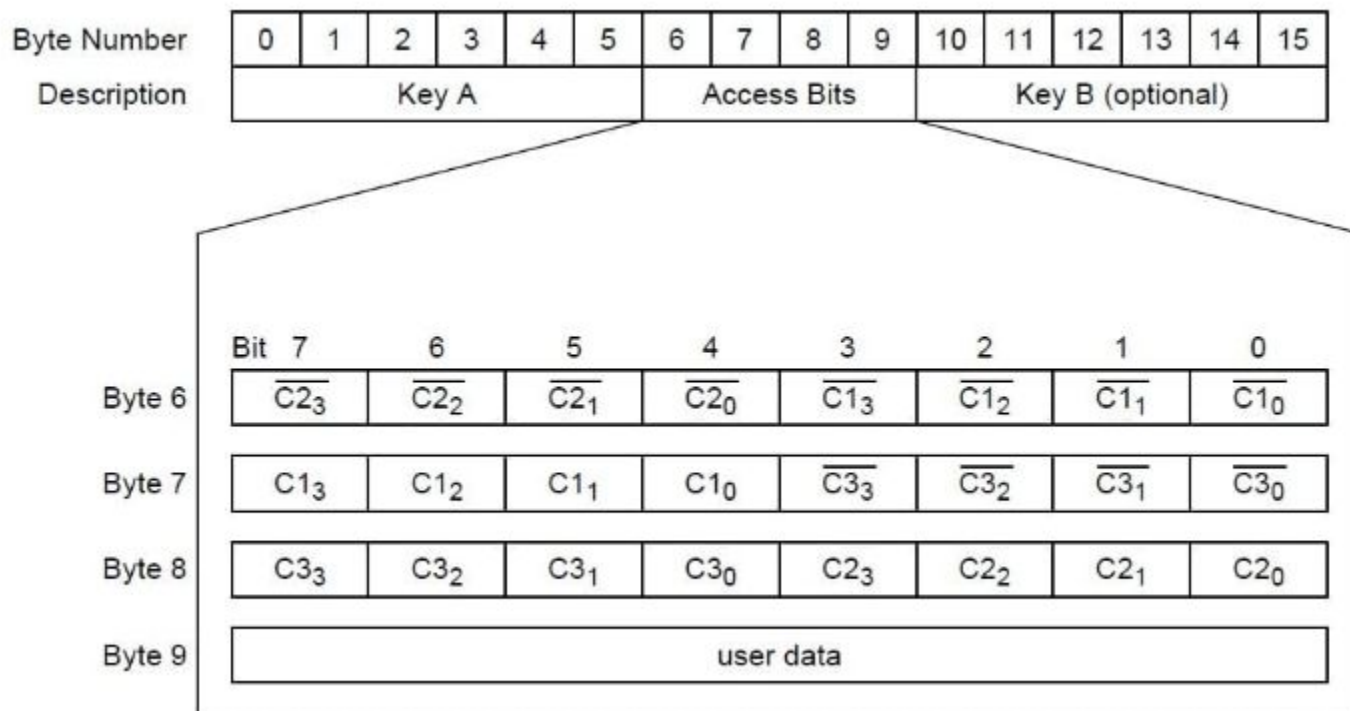
**UID** : Unique IDentifier

**LRC**: Longitudinal Redundancy Check on UID

**XX..XX**: Chip manufacturer reserved areas

# RFID Chips Mifare

- Estrutura de Memória (*Sector Trailer*):



# RFID Chips Mifare

“Garante” a segurança com:

- Chaves de acesso
- Criptografia (CRYPTO1)
  - Atualmente já foi quebrada;

# RFID Chips Mifare

- Implementação prática: Leitura e gravação de dados

```
/dev/ttyUSB0
|
***UFSM - Eng. de Computação***
---RFID - Controle
Selecione o modo leitura ou gravacao...

Recebi: read
Modo leitura selecionado
Aproxime o seu cartao do leitor...
UID da tag : 93 60 AC E5
NULL
NULL
---RFID - Controle
Selecione o modo leitura ou gravacao...

Recebi: write
Modo gravacao selecionado
Aproxime o seu cartao do leitor...
UID do Cartao: 93 60 AC E5nTipo do PICC: MIFARE 1KB
Digite o sobrenome,em seguida o caractere #
Digite o nome, em seguida o caractere #
Dados gravados com sucesso!
```

# RFID Chips Mifare

- Implementação prática: Dados atualizados

```

/dev/ttyUSB0
|
***UFSM - Eng. de Computação***
---RFID - Controle
Selecione o modo leitura ou gravacao...

Recebi: read
Modo leitura selecionado
Aproxime o seu cartao do leitor...
UID da tag : 93 60 AC E5
luis
dedeus
---RFID - Controle
Selecione o modo leitura ou gravacao...
```

# RFID Chips Mifare

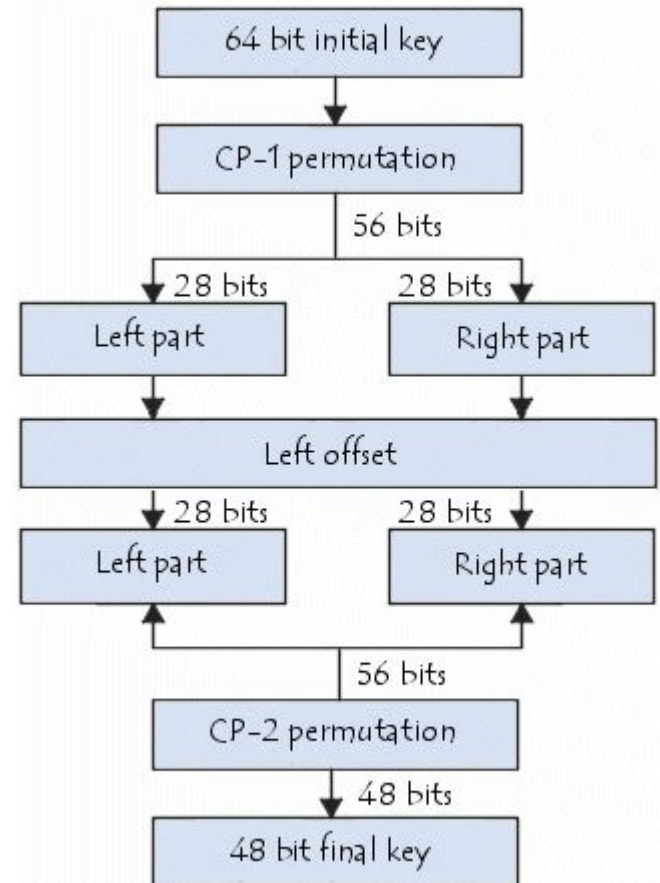
Implementação prática:  
Blocos de memória;

- Informação explícita bytes em hex (ASCII)

/dev/ttyUSB0															
9	39	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	38	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	37	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	36	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
8	35	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	34	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	33	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	32	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
7	31	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	30	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	29	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	28	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
6	27	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	26	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	25	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	24	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
5	23	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	22	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	21	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	20	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
4	19	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	18	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	17	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	16	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
3	15	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	14	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	13	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	12	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
2	11	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	10	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	9	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	8	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
1	7	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	6	00	00	00	00	00	00	00	00	00	00	00	00	00	[ 0 0 0 ]
	5	20	20	20	20	20	20	20	20	20	20	20	20	03	[ 0 0 0 ]
	4	0A	6C	75	69	73	66	65	6C	69	70	65	20	20	[ 0 0 0 ]
0	3	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	[ 0 0 1 ]
	2	20	20	20	20	20	20	20	20	20	20	20	20	03	[ 0 0 0 ]
	1	64	65	64	65	75	73	20	20	20	20	20	20	20	[ 0 0 0 ]
	0	93	60	AC	E5	BA	88	04	00	85	00	B4	2E	F0	[ 0 0 0 ]

# RFID Chips Mifare

- Implementação prática: Adicionar mais uma camada de criptografia;
- Usado algoritmo DES;
- Resultado 8 bytes de dados encriptados.





# RFID Chips Mifare

- Implementação prática: Criptografia DES

```
/dev/ttyUSB1
]
***UFSM - Eng. de Computação***
---RFID - Controle
Selecione o modo leitura ou gravacao...

Recebi: write
Modo gravacao selecionado
Aproxime o seu cartao do leitor...
UID do Cartao: 93 60 AC E5nTipo do PICC: MIFARE 1KB
Digite o sobrenome,em seguida o caractere #
108 l
117 u
105 i
115 s

===== DES ENCRYPT =====
108
117
105
115
108
117
105
115      nome encriptado
Encrypt...D6 62 62 28 A8 FF 71 57
Digite o nome, em seguida o caractere #
```

# RFID Chips Mifare

- Implementação prática:

/dev/ttyUSB1															
	50	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	49	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	48	00	00	00	00	00	00	00	00	00	00	00	00	00	00
11	47	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	46	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	45	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	44	00	00	00	00	00	00	00	00	00	00	00	00	00	00
10	43	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	42	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	41	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00
9	39	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	38	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	37	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	36	00	00	00	00	00	00	00	00	00	00	00	00	00	00
8	35	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	34	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	33	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	32	00	00	00	00	00	00	00	00	00	00	00	00	00	00
7	31	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	30	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	29	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	28	00	00	00	00	00	00	00	00	00	00	00	00	00	00
6	27	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	26	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	25	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	24	00	00	00	00	00	00	00	00	00	00	00	00	00	00
5	23	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	22	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	21	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00
4	19	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	18	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	17	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	16	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3	15	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	13	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	12	00	00	00	00	00	00	00	00	00	00	00	00	00	00
2	11	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	10	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	9	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	8	00	00	00	00	00	00	00	00	00	00	00	00	00	00
1	7	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	6	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	5	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E
	4	0A	62	62	28	A8	FF	71	57	20	20	20	20	20	20
0	3	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF
	2	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E
	1	D6	62	62	28	A8	FF	71	57	20	20	20	20	20	20
	0	93	60	AC	E5	BA	88	04	00	85	00	B4	2E	F0	BB

# RFID Chips Mifare

## Implementação prática: Decodificação usando site

### DES – Symmetric Ciphers Online

Input type:

Text

Input text:  
(hex)

D6 62 62 28 A8 FF 71 57

☐ Plaintext ☒ Hex

Autodetect: **ON** | OFF

Function:

DES

Mode:

ECB (electronic codebook)

Key:  
(plain)

3b 38 98 37 15 20 f7 5e

☐ Plaintext ☒ Hex

> Encrypt!

> Decrypt!



Decrypted text:

00000000

6c 75 69 73 21 c5 00 00

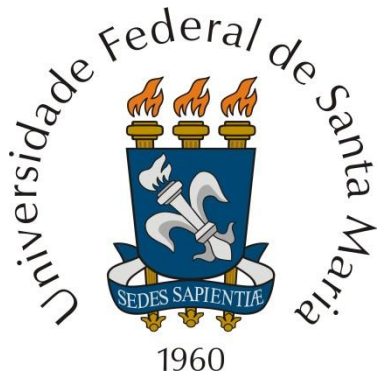
l u i s ! Å . .

# Conclusão

- Tecnologia já consolidada, mas segue evoluindo;
- Alta empregabilidade na otimização de processos;
- Áreas com pouca influência da tecnologia já adotam sistemas com RFID (Pecuária, fazendas, mercados).
- A Segurança em relação ao RFID não é algo consolidado e possui vulnerabilidades;

# Obrigado pela Atenção !

## Perguntas?



Luis Felipe de Deus – [dedeus.f.l@gmail.com](mailto:dedeus.f.l@gmail.com)