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

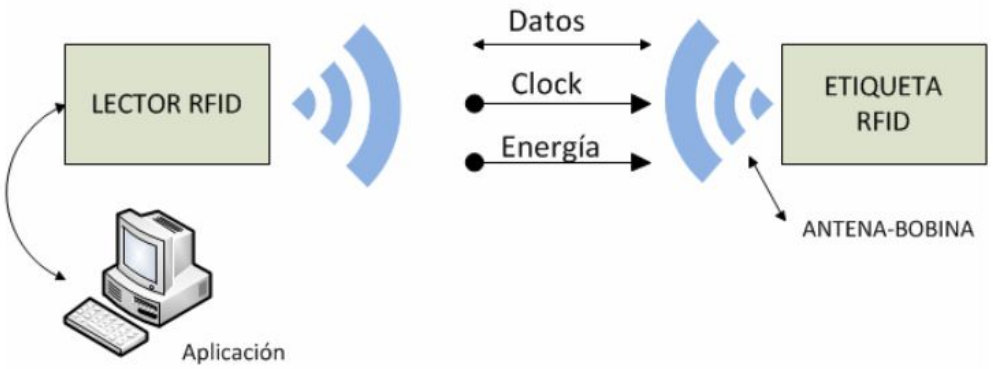
Radio-Frequency Identification (RFID)

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

Dezembro/2019

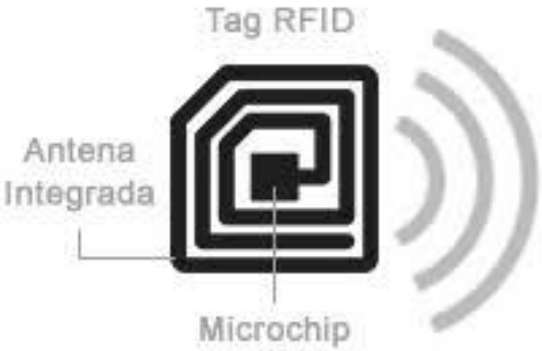
Introdução

- 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

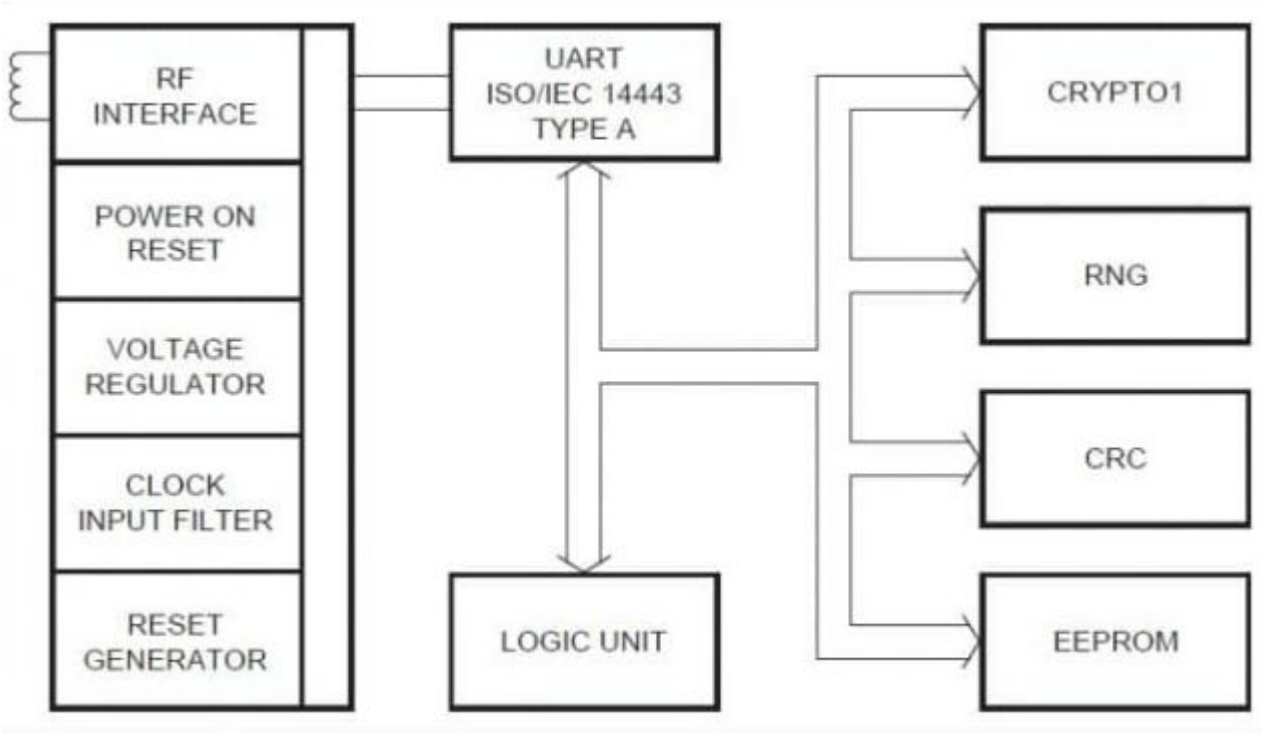
- Criptografia;
- Chaves de acesso;
- Blindagem eletromagnética;
- Modulação.

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

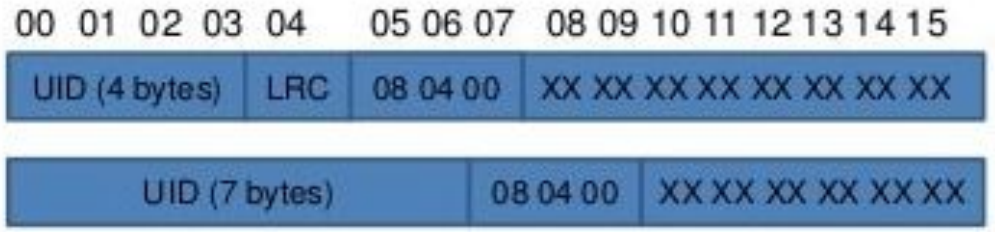
- Diagrama de Blocos:



RFID Chips Mifare

Estrutura de Memória:

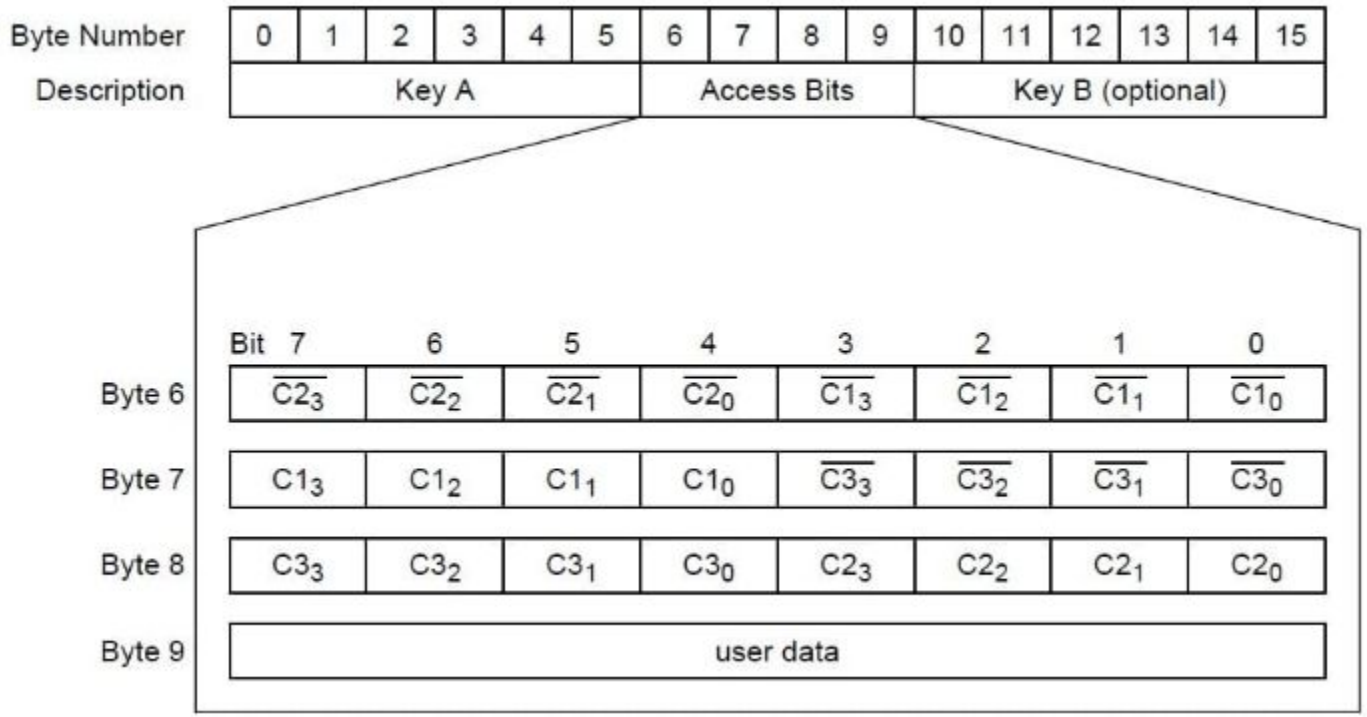
- Divididos em setores;
- Setores divididos em blocos;
- Cada bloco possui 16 bytes.



UID : Unique IDentifier
LRC: Longitudinal Redundancy Check on UID
XX..XX: Chip manufacturer reserved areas

RFID Chips Mifare

- Estrutura de Memória (*Sector Trailer*):



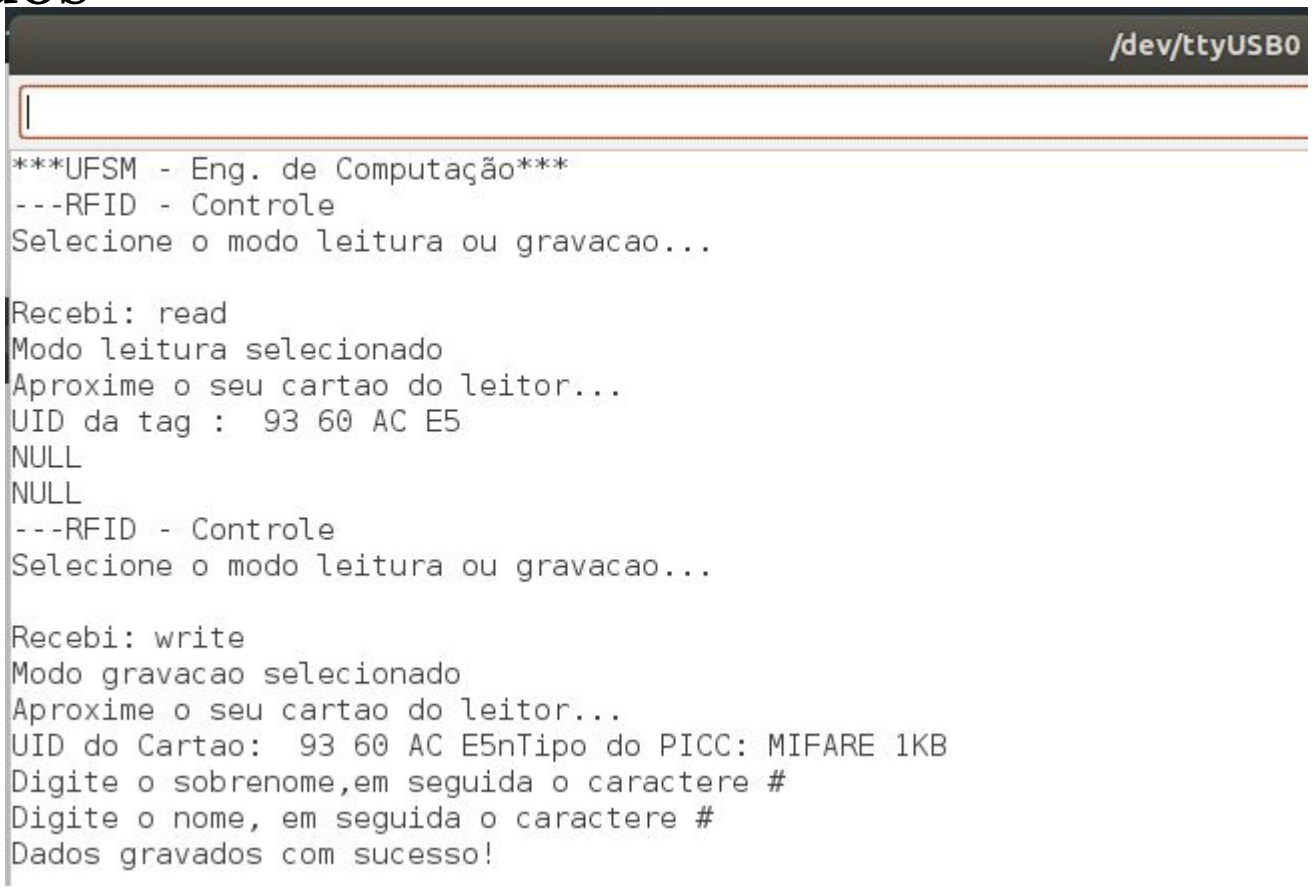
RFID Chips Mifare

“Garante” a segurança com:

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

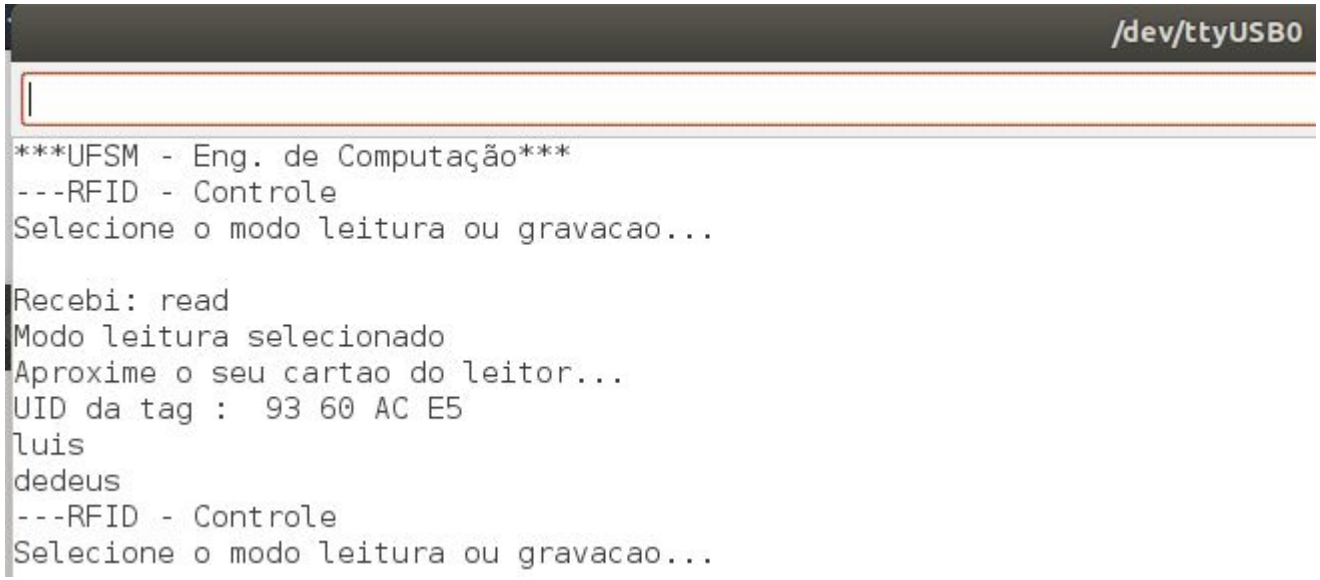
RFID Chips Mifare

- Implementação prática: Leitura e gravação de dados



RFID Chips Mifare

- Implementação prática: Dados atualizados

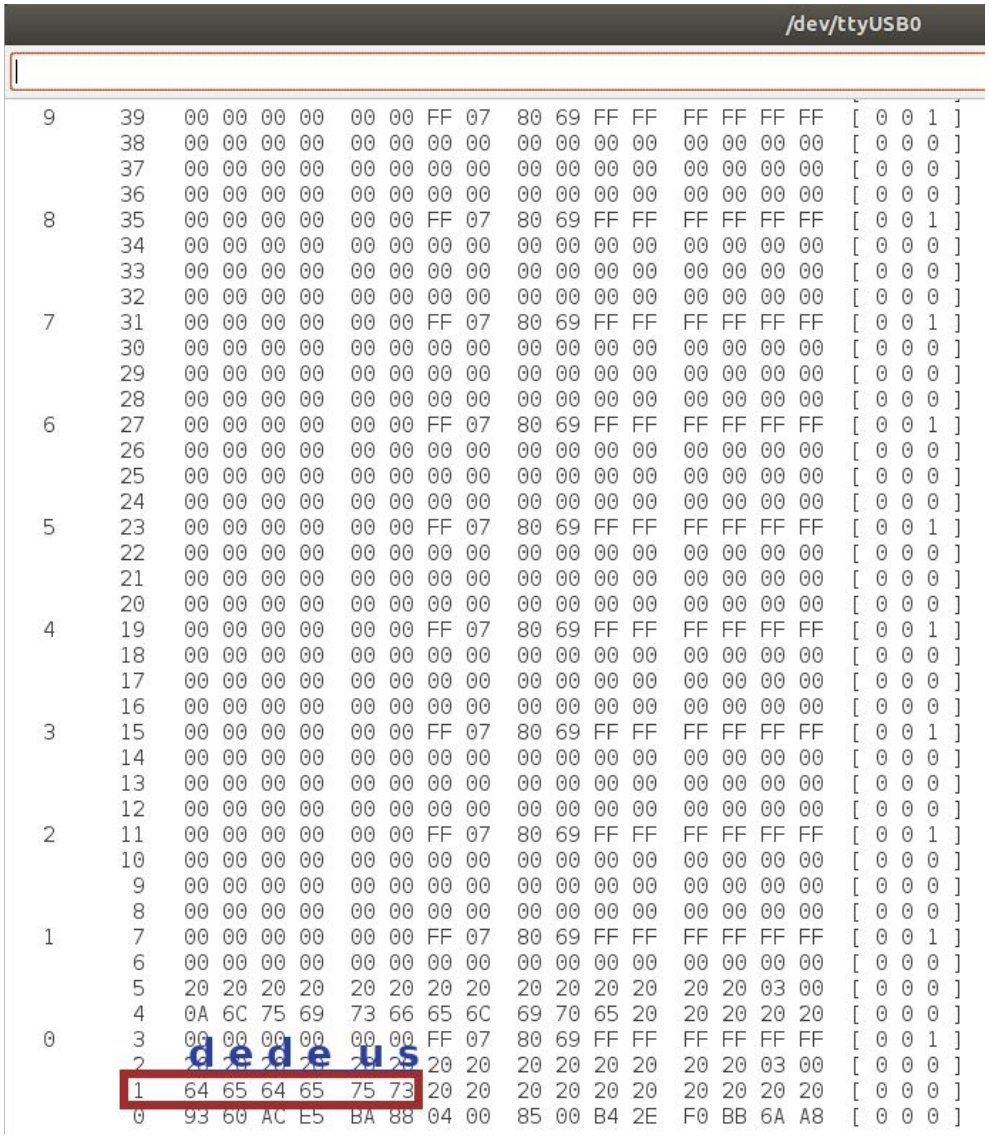


RFID Chips Mifare

Implementação prática: Blocos de memória;

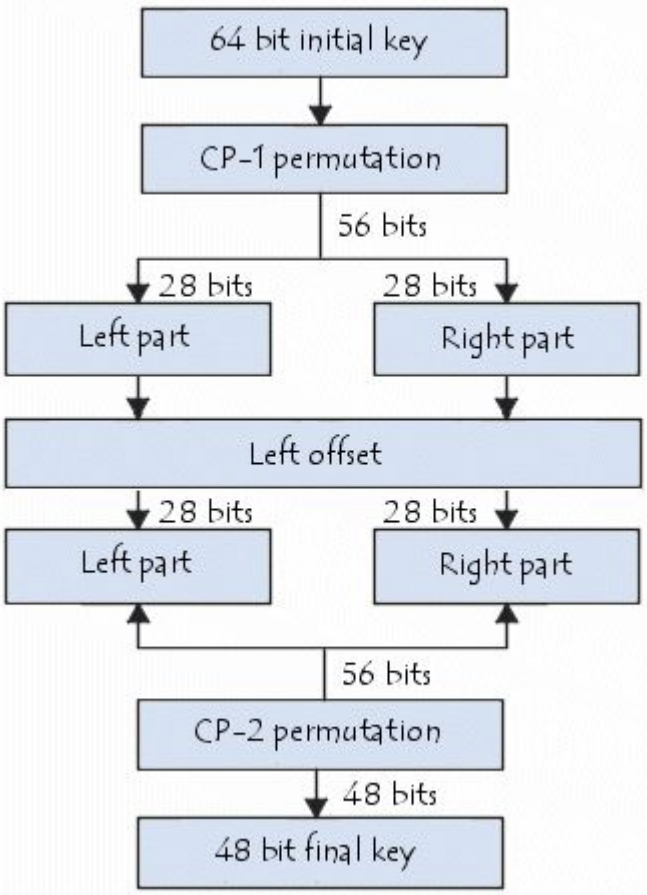
- Informação explícita

bytes em hex (ASCII)



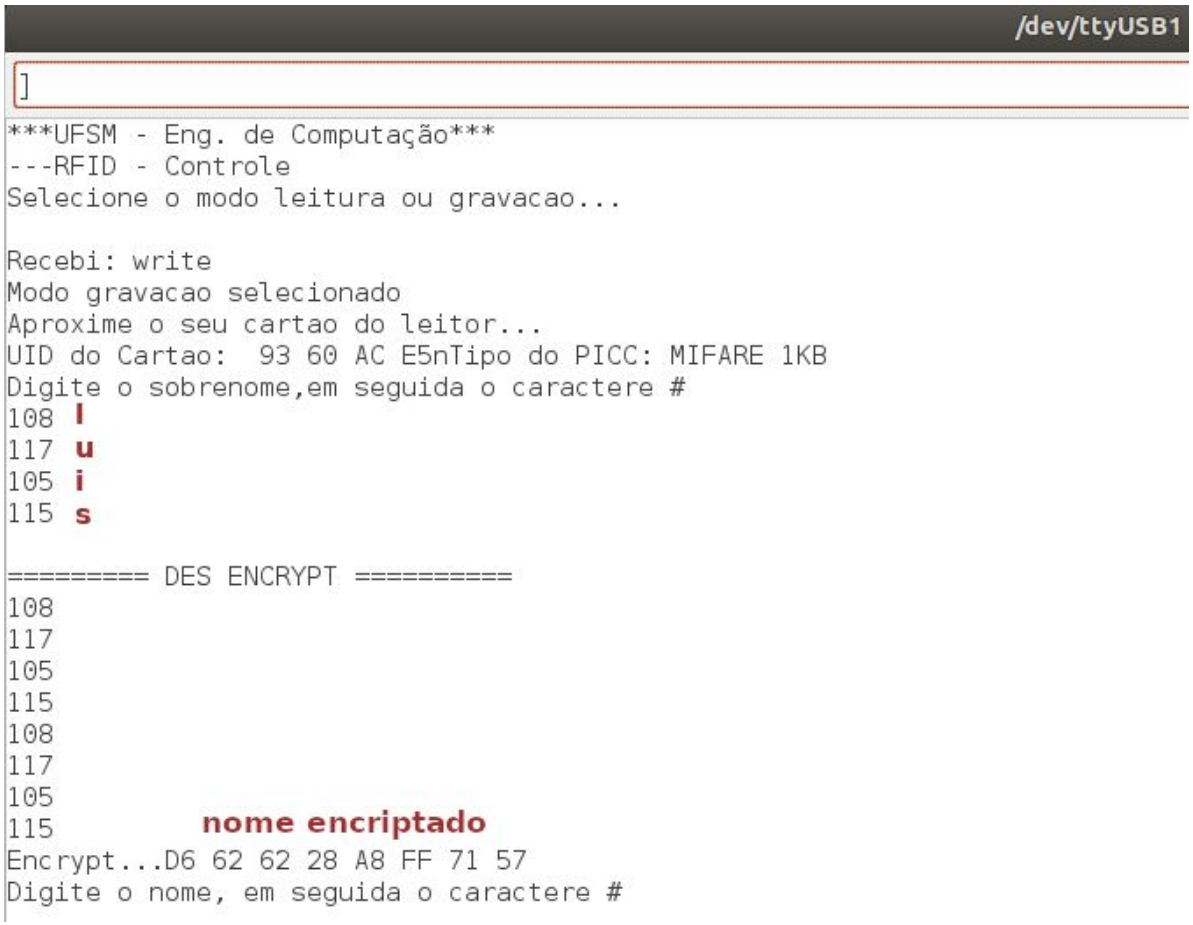
RFID Chips Mifare

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



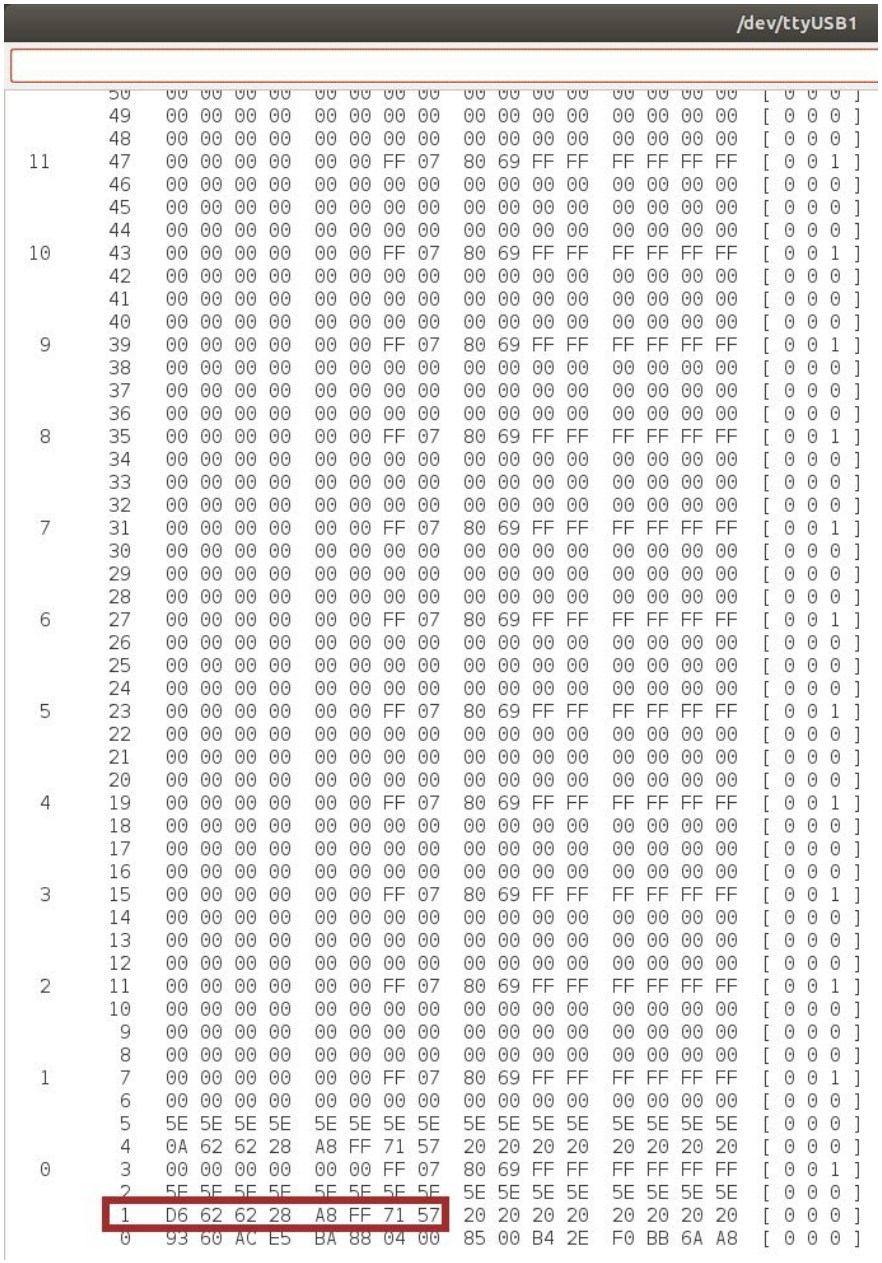
RFID Chips Mifare

- Implementação prática: Criptografia DES



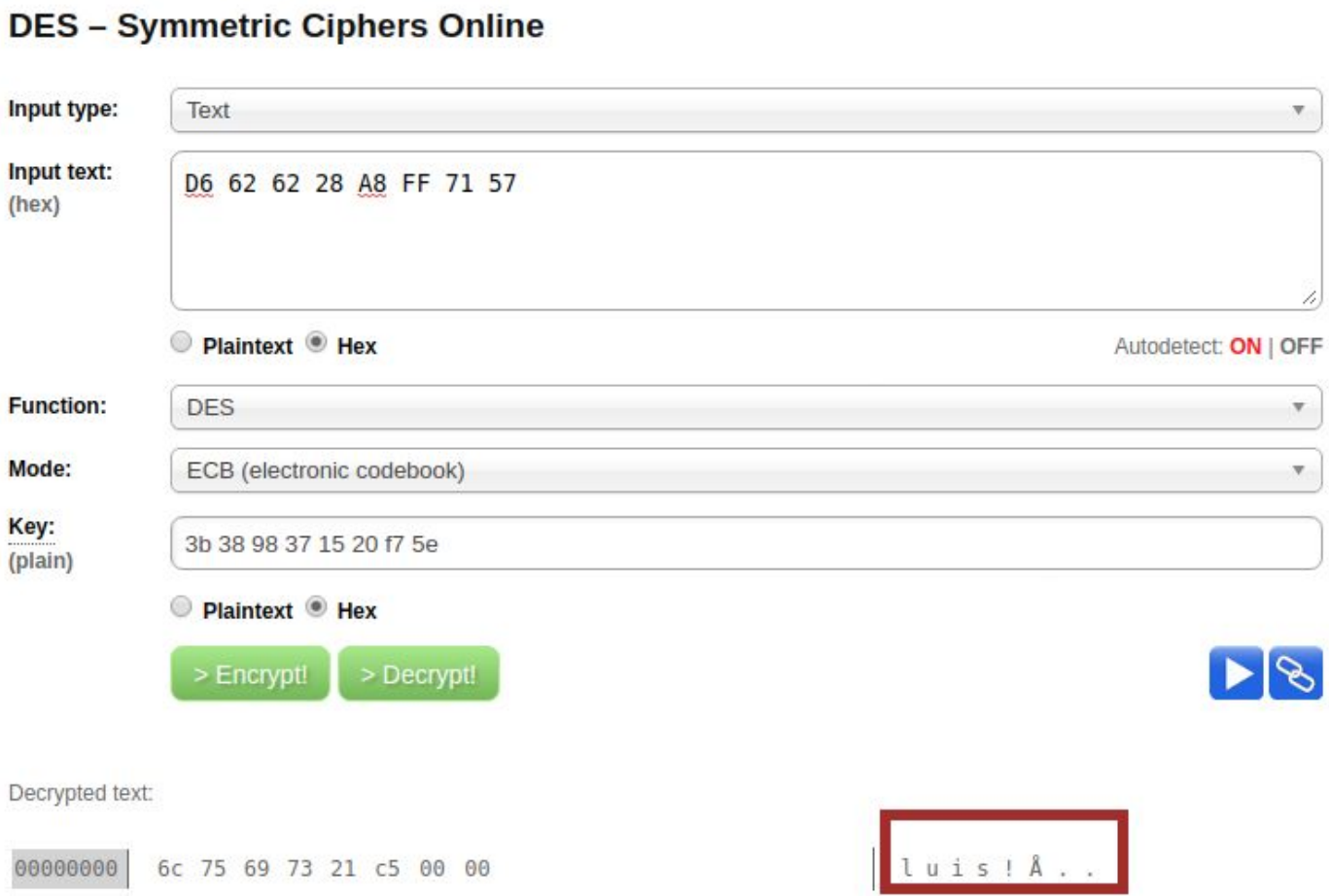
RFID Chips Mifare

- Implementação prática:



RFID Chips Mifare

Implementação prática: Decodificação usando site

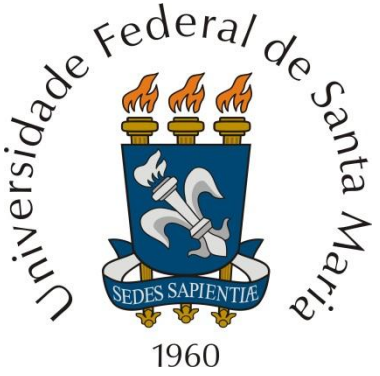


Conclusão

- 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