Estruturas Criptográficas

Criptografia e Segurança da Informação

TP1 - Exercício 1 - Grupo 3

Packages Utilizados

- ascon
- random
- hashlib
- asyncio
- nest_asyncio

Criação da Chave

A seed para a chave é introduzida pelo utilizador.

```
key_seed=input("Seed for key > ")
```

Criação da chave com recurso à função de hash que utiliza o algoritmo `Ascon-Xof`

```
key=ascon.hash(key_seed.encode(),variant="Ascon-Xof", hashlength=hashlength)
```

Criação do *Nounce*

Obter 128 bits para geração do nounce

```
nounce_seed=str(random.getrandbits(128))
```

Gerar o *nounce* desejado recorrendo à função de hash que utiliza o algoritmo `Ascon-Xof`

```
nounce=ascon.hash(nounce_seed.encode(),variant="Ascon-Xof", hashlength=hashlength)
```

Criação da *Associated Data*

Obter a hash da mensagem a ser enviada

```
sha256_hash = hashlib.sha256(in_message).hexdigest()
```

Processo de Envio da Mensagem

- Criação do *nounce*
- Criação da *associated data*
- Cifrar o texto original utilizando `Ascon-128`

```
out_message=ascon.encrypt(key, nounce, associated_data, in_message.encode(), variant="Ascon-128")
```

- Adicionar os dados a ser enviados à queue

```
queue.put(out_message,nounce,associated_data)
```

Processo de Receção da Mensagem

- Receção da mensagem, *nounce* e *associated data* da queue

```
message, nounce, associated_data = await queue.get()
```

- Verificar se o *nounce* é válido, i.e., se nunca foi utilizado
- Decifrar a mensagem utilizando `Ascon-128`

```
out_message=ascon.decrypt(key, nounce, associated_data, text, variant="Ascon-128")
```

Processo de Receção da Mensagem

- Verificar se a mensagem recebida foi decifrada com sucesso

```
if out_message == None: return "[ERROR] Decryption failed"
```

- Verificar se a hash da mensagem recebida é igual à hash da mensagem original

```
if calculate_sha256(out_message.decode()) != associated_data.decode():
    return "[ERROR] Message has been tampered"
```

Processo de Execução

- Criação de uma queue para envio e receção de mensagens
- Obter a seed para a chave com input do utilizador
- Gerar a chave recorrendo à função de hash que utiliza o algoritmo `Ascon-Xof`
- Iniciar o processo de envio e receção de mensagens
- Aguardar que ambos os processos terminem

Possiveis Vulnerabilidades

- Ataques por repetição
  - Resolvido com a verificação do *nounce* único para cada mensagem
- Ataques por alteração da mensagem
  - Resolvido com a verificação da hash da mensagem recebida presente na *associated data*

Estruturas Criptográficas

Criptografia e Segurança da Informação

TP1 - Exercício 1 - Grupo 3