**CRYPTOGRAPHY AND COMPUTER SECURITY**

**BİL 470**

**Berkan AKIN**

**171044073**

**ASCON (Authenticated Stream Cipher with No Leakage)**

ASCON (Authenticated Stream Cipher with No Leakage) is a lightweight authenticated encryption algorithm designed to provide security against known and chosen-key attacks. It was designed by a team of researchers from the Technical University of Denmark and the Università degli Studi di Milano in 2016.

ASCON is a stream cipher that uses a permutation-based construction and a sponge-based mode of operation. It takes a secret key and a nonce as input, and generates a pseudorandom keystream from them. The keystream is then used to encrypt and authenticate a message using the encrypt-then-MAC paradigm. ASCON has a security proof based on the assumption that the underlying permutation is a random function, and is resistant to a wide range of attacks, including differential and linear cryptanalysis, key recovery attacks, and fault attacks.

ASCON is suitable for a variety of applications, including secure messaging, key exchange, and file encryption. It is fast, has a low memory footprint, and has a simple design, making it easy to implement and deploy. It is available as an open-source library in a number of programming languages, including C, C++, Go, and Rust.

**ISAP**  **(Improved Simple Authenticated Permutation)**

ISAP (Improved Simple Authenticated Permutation) is a permutation-based authenticated encryption with additional data (AEAD) scheme that provides security against a wide range of implementation attacks, such as differential fault attacks, statistical fault attacks, statistical ineffective fault attacks, and differential power analysis. It was designed by a team of researchers from the Technical University of Denmark in 2020.

ISAP uses a nonce-based encrypt-then-MAC construction, where the encryption is done by XORing a message and a keystream, and the authentication/verification is based on a hash-then-MAC paradigm. It takes a secret key and a nonce as input, and generates a keystream from them using a permutation-based construction. The keystream is then used to encrypt and authenticate the message. ISAP has a security proof based on the assumption that the underlying permutation is a random function, and is resistant to a wide range of attacks, including differential and linear cryptanalysis, key recovery attacks, and fault attacks.

ISAP is suitable for a variety of applications, including secure messaging, key exchange, and file encryption. It is fast, has a low memory footprint, and has a simple design, making it easy to implement and deploy. It is available as an open-source library in a number of programming languages, including C, C++, Go, and Rust.

**Compare ASCON (Authenticated Stream Cipher with No Leakage) and ISAP (Improved Simple Authenticated Permutation)**

ASCON (Authenticated Stream Cipher with No Leakage) and ISAP (Improved Simple Authenticated Permutation) are both lightweight authenticated encryption algorithms designed to provide security against known and chosen-key attacks. Both algorithms use a permutation-based construction and a sponge-based mode of operation, and take a secret key and a nonce as input.

One key difference between ASCON and ISAP is the way in which they generate and use the keystream. ASCON is a stream cipher that generates a keystream from the secret key and the nonce, and uses the key stream to encrypt and authenticate the message using the encrypt-then-MAC paradigm. ISAP, on the other hand, uses a permutation-based construction to generate a keystream from the secret key and the nonce, and uses the keystream to encrypt and authenticate the message.

Another difference between ASCON and ISAP is their security proofs. ASCON has a security proof based on the assumption that the underlying permutation is a random function, and is resistant to a wide range of attacks, including differential and linear cryptanalysis, key recovery attacks, and fault attacks. ISAP also has a security proof based on the assumption that the underlying permutation is a random function, and is specifically designed to provide security against a wider range of implementation attacks, such as differential fault attacks, statistical fault attacks, statistical ineffective fault attacks, and differential power analysis.

Both ASCON and ISAP are suitable for a variety of applications, including secure messaging, key exchange, and file encryption. They are fast, have a low memory footprint, and have a simple design, making them easy to implement and deploy. They are available as open-source libraries in a number of programming languages, including C, C++, Go, and Rust.

**Comparesion Table**

| **Feature** | **ASCON** | **ISAP** |
| --- | --- | --- |
| Algorithm type | Stream cipher | Permutation-based AEAD |
| Key size | 128 bits | 128 bits |
| Nonce size | 128 bits | 128 bits |
| Keystream generation | Pseudorandom permutation | Permutation-based construction |
| Encryption | Encrypt-then-MAC | Encrypt-then-MAC |
| Security proof | Random permutation assumption | Random permutation assumption |
| Resistance to attacks | Differential and linear cryptanalysis | Differential fault, statistical fault, and differential power analysis |
| Applications | Secure messaging, key exchange, file encryption | Secure messaging, key exchange, file encryption |
| Implementation languages | C, C++, Go, Rust.Python | C, C++, Go, Rust,Python |

**Note**: isab cbc function not working, Hash functions are missing for ascon. not made for isab. Just run the given functions for the homework