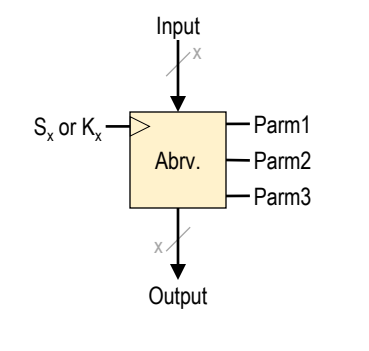
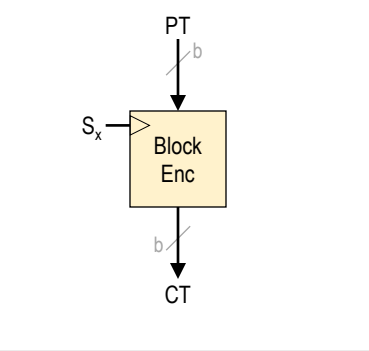


HVOC Summary // Hacking Vehicle On-board Communications / ABE 590 / Spring 2023

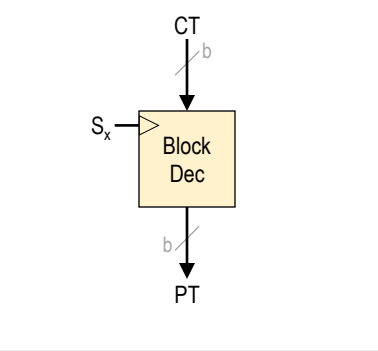
Name: example1, example2, ...



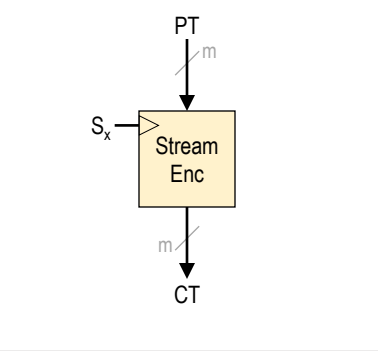
Block Encrypt: AES, Salsa20, Blowfish



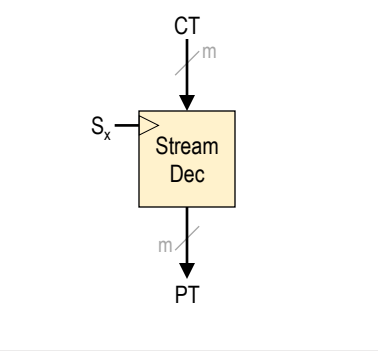
Block Decrypt: AES, Salsa20, Blowfish



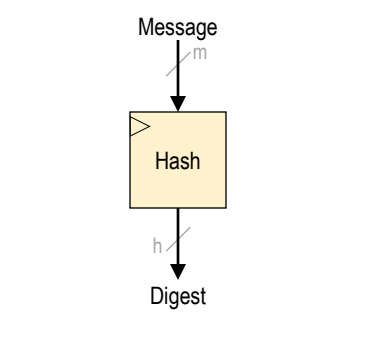
Stream Encrypt: AES-CTR



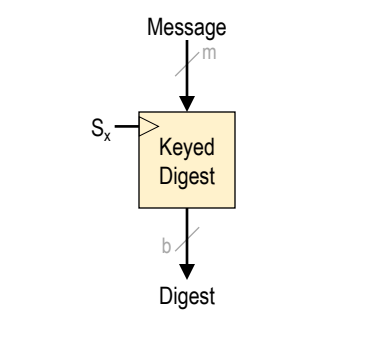
Stream Decrypt: AES-CTR



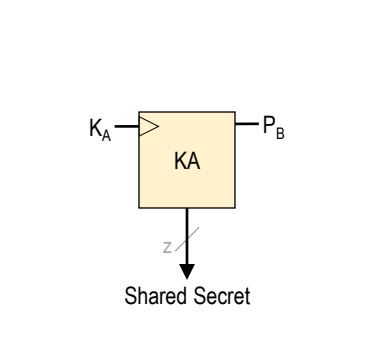
Hash: SHA256, SHA512, SHA512/256



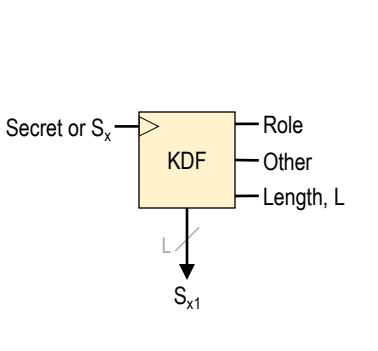
Keyed Digest: AES-CMAC



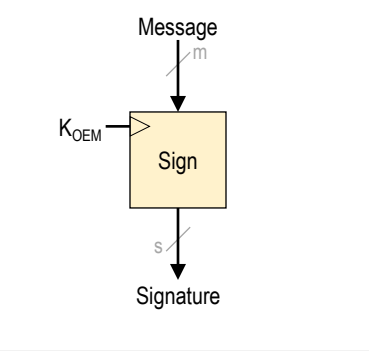
Key Agreement: X25519



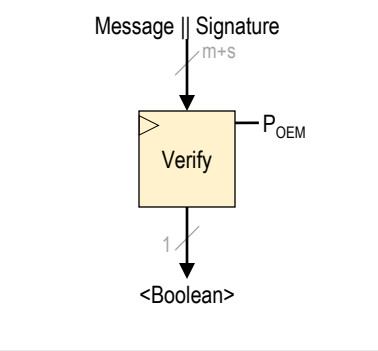
Key Derivation Function: HKDF



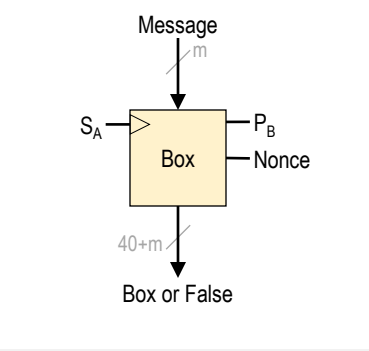
Sign: Ed25519



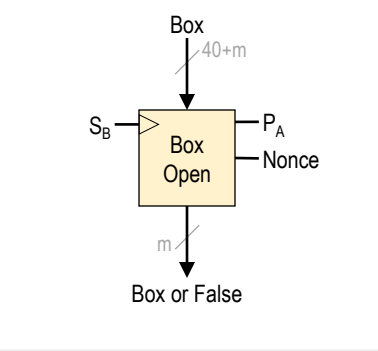
Verify: Ed25519



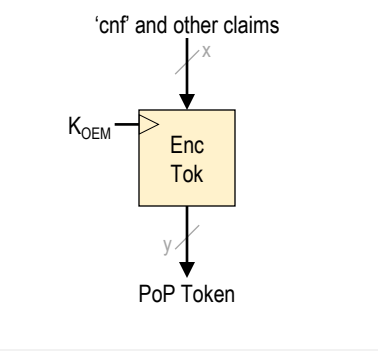
Box: NaCl box()



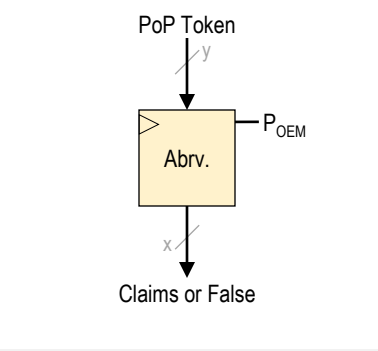
Box Open: NaCl box_open()



Encode Token: CWT



Decode Token: CWT



Inputs

- **PT** – plaintext
- **CT** – ciphertext
- **Message** – message, not related to encryption. (Could argue that PT is also valid, but PT is usually reserved for situations where encryption is involved. That is, when there is also going to be a CT.)
- **Signature** – used to verify message
- **Box** – binary “blob” generated by NaCl box()
- **‘cnf’** – confirmation claim (the public key of the ECU using the token)
- **Claims** – other token claims
- **PoP Token** – binary “blob” in a specific token format that supports proof-of-possession.

Input Sizes

- **b** – blocksize
- **m** – message size
- **s** – length of signature
- **x** – length of claims before being put into token
- **y** – length of encoded token

Keys / Secrets

- **S_X** – symmetric key for entity X
- **P/K_A** – Alice’s public/private keypair
- **P/K_B** – Bob’s public/private keypair
- **P/K_{OEM}** – OEM’s public/private keypair
- **Shared Secret** – Information intended to be kept secret and used to generate symmetric keys

Non-Key Parameters

- **Role** – the intended role the derived key is for
- **Other** – other input to KDF
- **Length** – desired size of key created by KDF
- **Nonce** – number used once to ensure boxed data is unique, even if message and keys are used repetitively

Outputs (not included above)

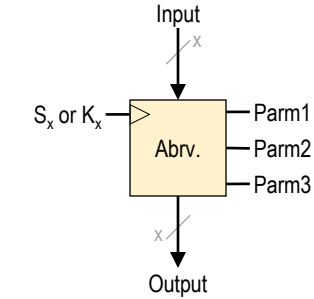
- **Digest** – fixed size “fingerprint” of (arbitrary size) message
- **S_{X1}** – the derived key
- **<Boolean>** – ‘true’ when received message is verified by signature, ‘false’ otherwise

Output Sizes (not included above)

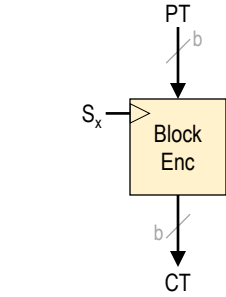
- **h** – hash size
- **z** – size of shared secret from key agreement function
- **L** – size of derived key

HVOC Summary // Hacking Vehicle On-board Communications / ABE 590 / Spring 2023

Name: example1, example2, ...

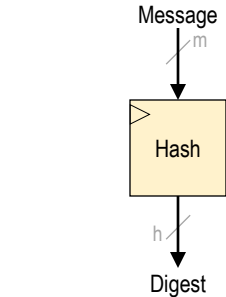


Block Encrypt: AES, Salsa20, Blowfish



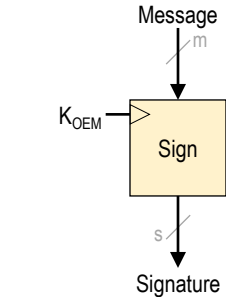
NIST 800-38A

Hash: SHA256, SHA512, SHA512/256



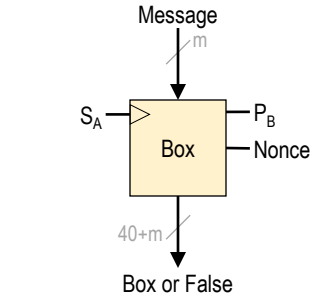
FIPS 180-4

Sign: Ed25519



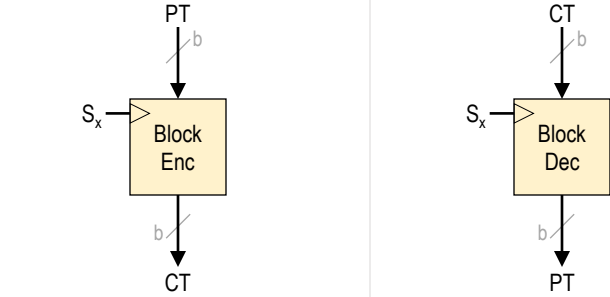
RFC 8032

Box: NaCl box()



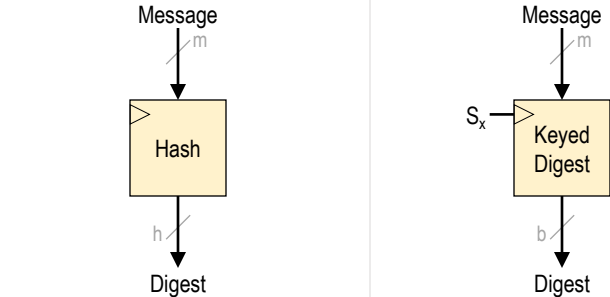
<https://tweetnacl.cr.yp.to>

Block Decrypt: AES, Salsa20, Blowfish



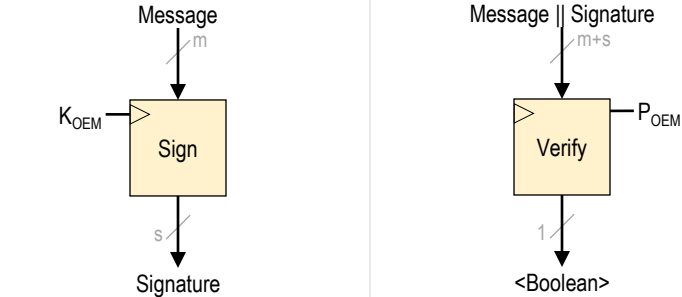
NIST 800-38A

Keyed Digest: AES-CMAC



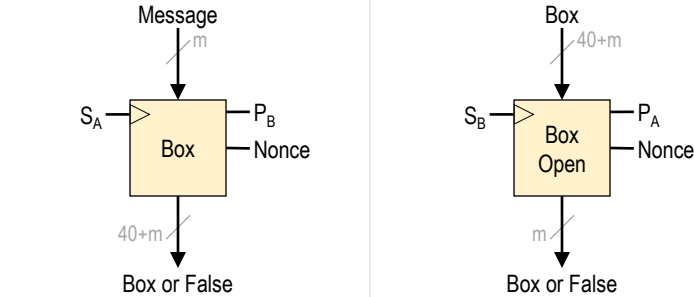
RFC 4493, NIST 800-38B

Verify: Ed25519



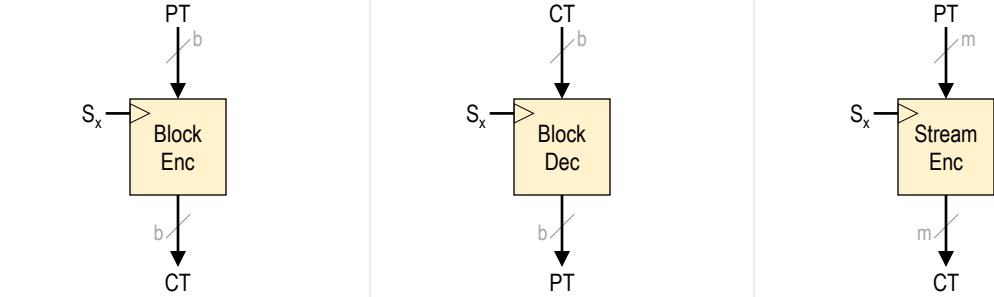
RFC 8032

Box Open: NaCl box_open()



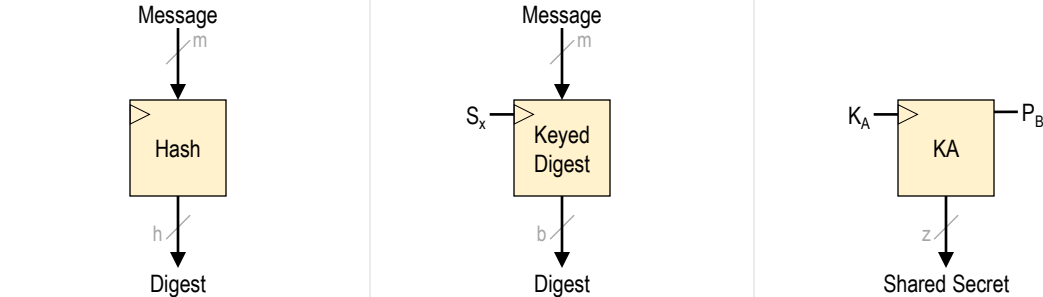
<https://tweetnacl.cr.yp.to>

Stream Encrypt: AES-CTR



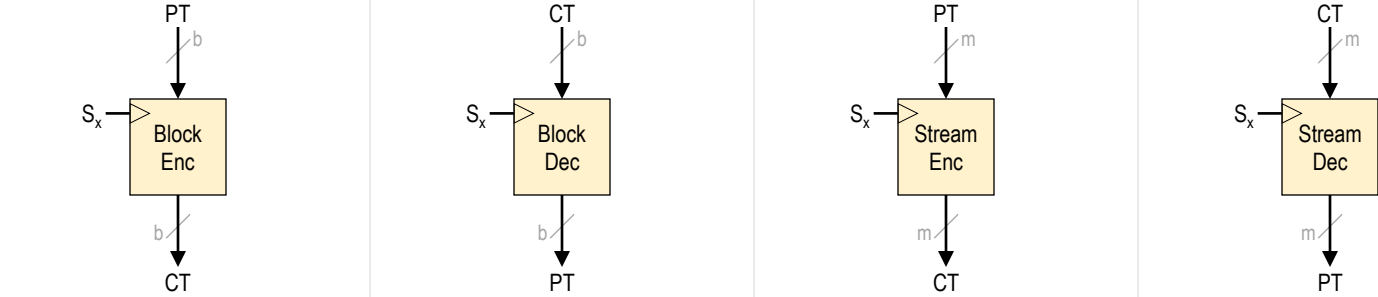
NIST 800-38A

Key Agreement: X25519



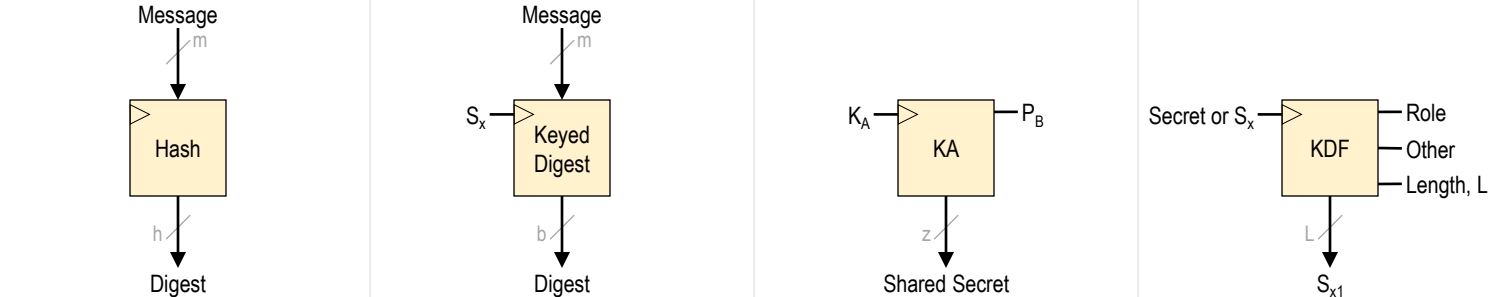
RFC 7748

Stream Decrypt: AES-CTR



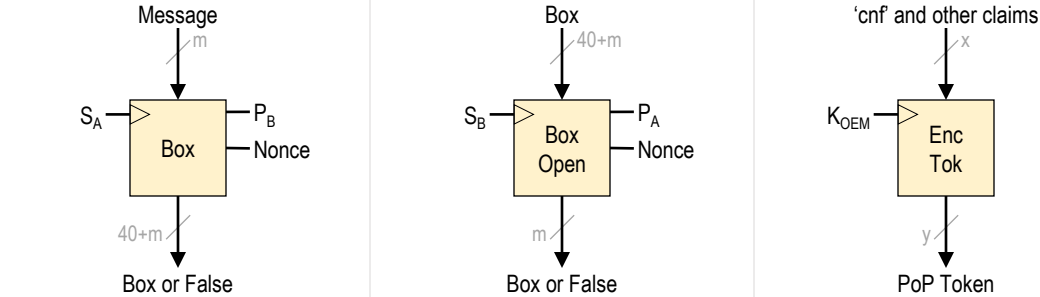
NIST 800-38A

Key Derivation Function: HKDF



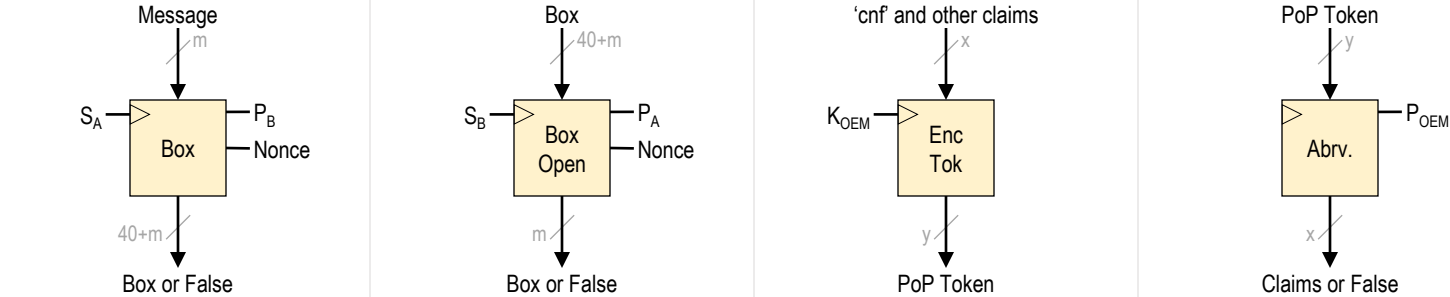
NIST 800-56Ar2

Encode Token: CWT



RFC 8949, 8392, 7800,

Decode Token: CWT



RFC 8949, 8392, 7800,