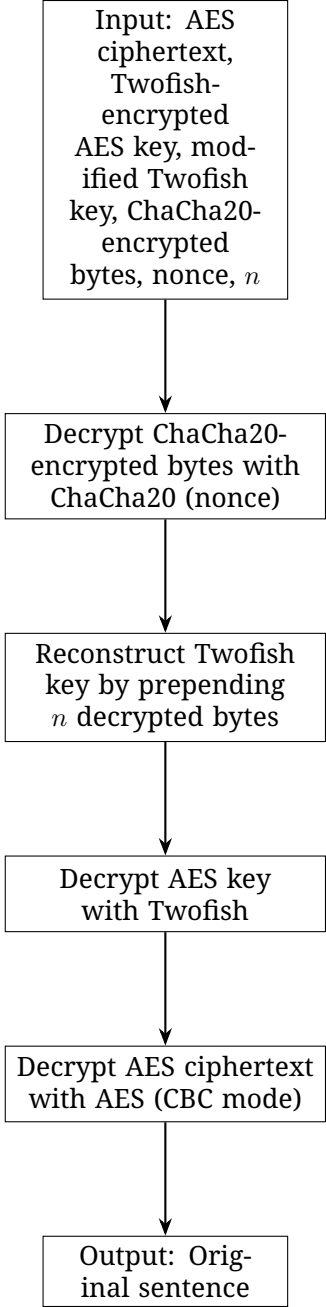


Input: AES ciphertext, Twofish-encrypted AES key, modified Twofish key, ChaCha20-encrypted bytes, nonce,  $n$



```
graph TD; A[Input: AES ciphertext, Twofish-encrypted AES key, modified Twofish key, ChaCha20-encrypted bytes, nonce, n] --> B[Decrypt ChaCha20-encrypted bytes with ChaCha20 (nonce)]; B --> C[Reconstruct Twofish key by prepending n decrypted bytes]; C --> D[Decrypt AES key with Twofish]; D --> E[Decrypt AES ciphertext with AES (CBC mode)]; E --> F[Output: Original sentence];
```

Decrypt ChaCha20-encrypted bytes with ChaCha20 (nonce)

Reconstruct Twofish key by prepending  $n$  decrypted bytes

Decrypt AES key with Twofish

Decrypt AES ciphertext with AES (CBC mode)

Output: Original sentence