Applied Cryptography

Lecture 3

Arnab Roy

20 March

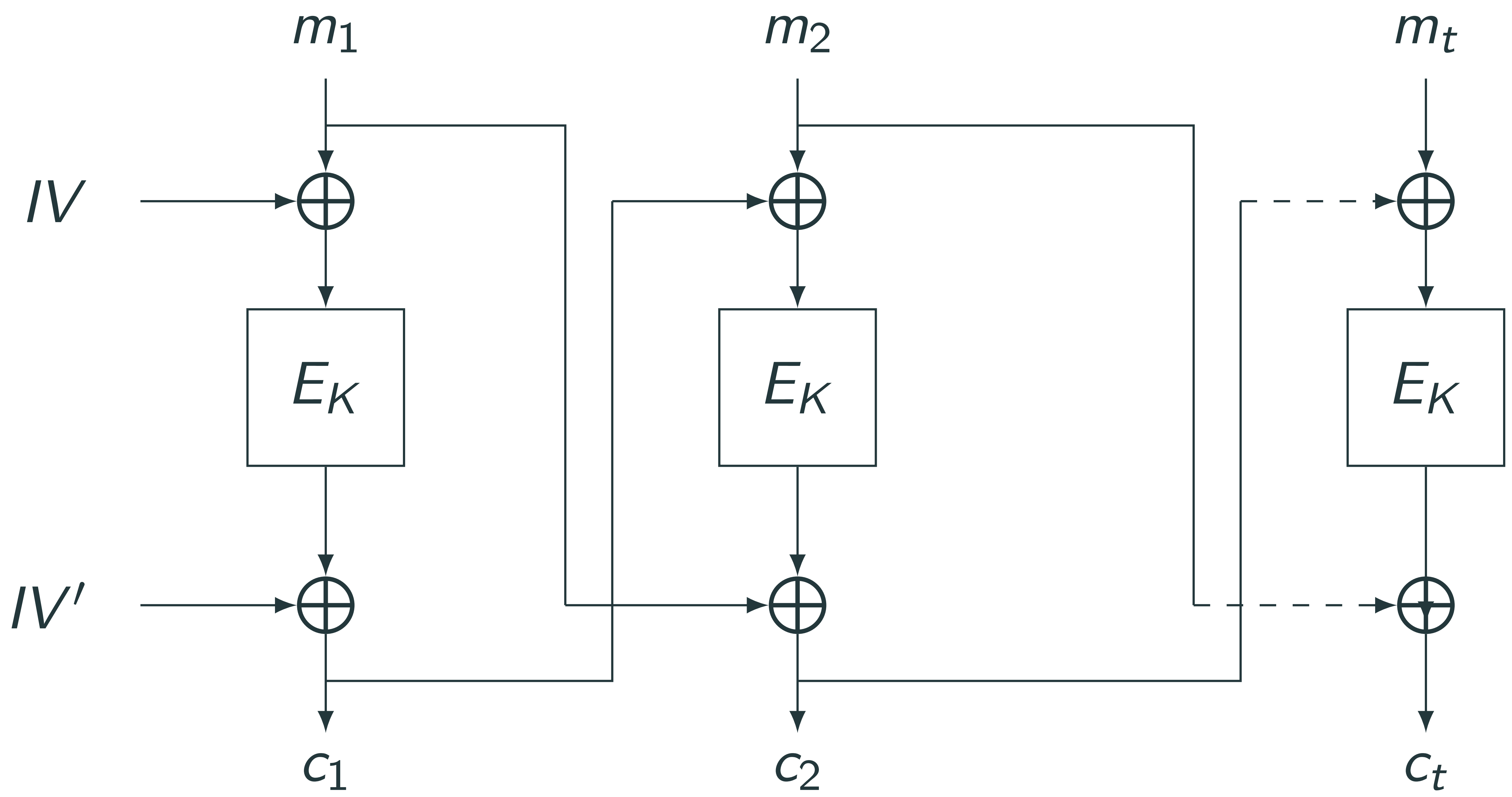
University of Innsbruck

Recall: Block Cipher and Encryption Mode

- What is the main purpose of a block cipher in cryptographic security?
- Mathematical characterisation of a block cipher
  - What kind of function is E_K when K is fixed to a value say k?
  - What kind of function is E when both K and input m can vary?
  - What kind of function $E(\cdot, m)$ when input m is fixed to m_0 and K can vary?
- Given a plaintext ciphertext pair (m, c) where $c = E_K(m)$ can you think of a simple way to recover the secret key K
- Why do we need encryption mode? What does it achieve?

For answers to the above questions refer to the explanations on board during the lecture

IGE (Infinite Garble Extension) Encryption Mode



- Has two initial values IV, IV'
- Original proposal chooses IV randomly and $IV' = E_K(IV)$
- OpenSSL implementation: IV, IV' are provided by the user

IGE Encryption Mode

Cloud chat (server-client encryption)

- Data for encryption consists of *salt (64 bit) , session id (64 bit) payload, padding (12-1024 bytes)*
- *Payload* always contains *time*, *length* and *sequence number* which are checked by the receiver after decryption
- Encryption is done with IGE mode instantiating the block cipher with AES-256

Secret chat (end-to-end encryption)

- Data for encryption contains *Length (32 bit), Payload type (32 bit), random bytes (minimum128 bit), Layer (32 bit), IN_seq_no (32 bit) , OUT_seq_no (32 bit), message type (32 bit), serialised message object (variable length), Padding (12-1024 bytes)*
- Payload contains other aspects as mentioned in the Cloud chat case

More on the Telegram protocol in latter lectures (after introduction of *public key cryptography*)

For more details on the Telegram protocols check

1. https://core.telegram.org/mtproto
2. https://core.telegram.org/api/end-to-end

THANK YOU!