Convergent Encryption

Business Continuity

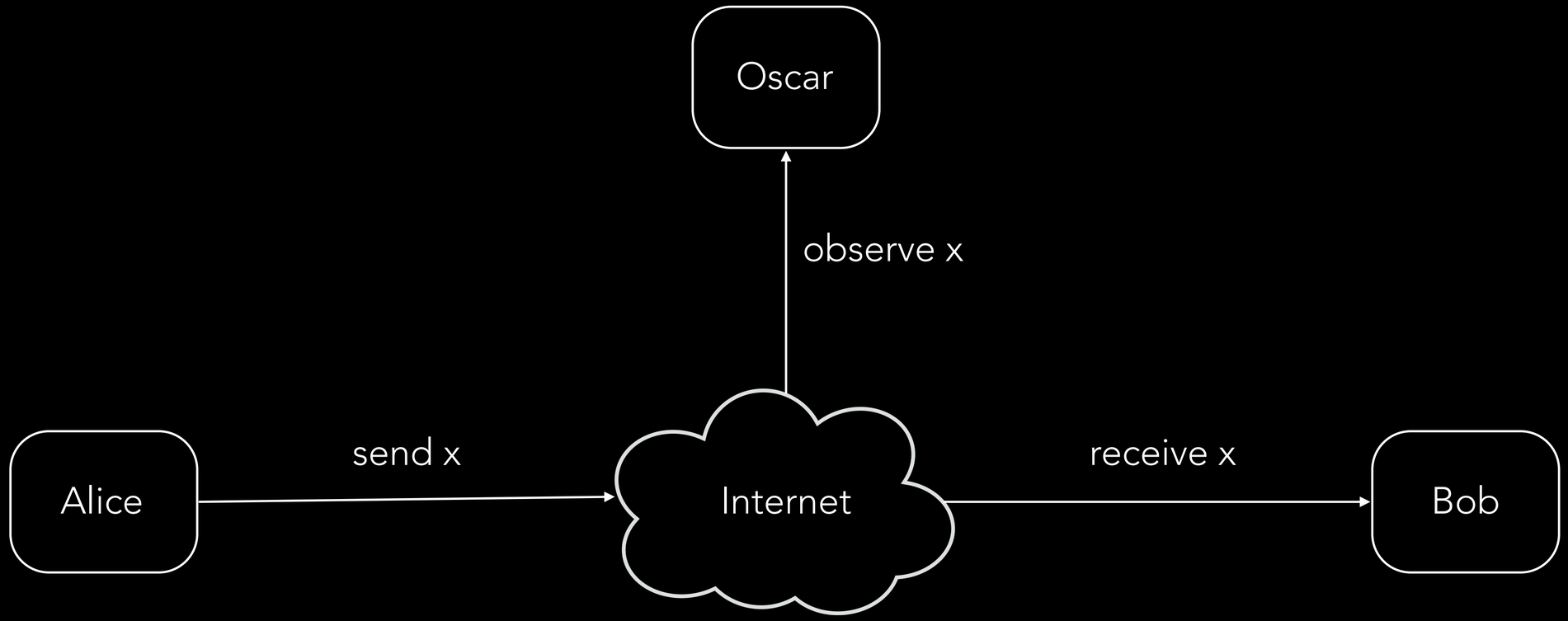
Data security

Encryption

- Encryption is a process that can be used to ensure the confidentiality of data, ensuring only those that are authorised can consume data.
- The aim of encryption is to readable binary data or **plain text** and use the process to convert the data into a non-readable form or **cipher text**.
- There are many different approaches and strategies to the encryption process and the optimal approach depends on-part on the context.

Data security

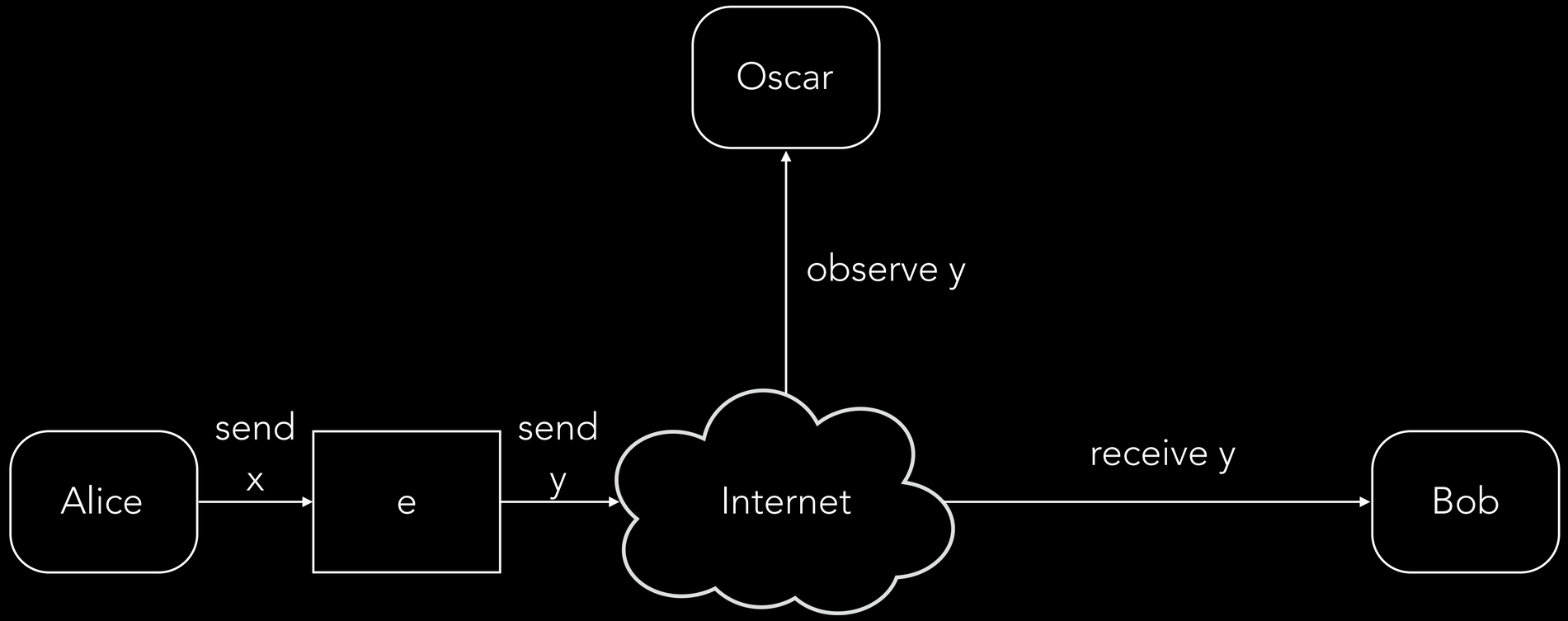
Convergent encryption



Symmetric-key crypto-system

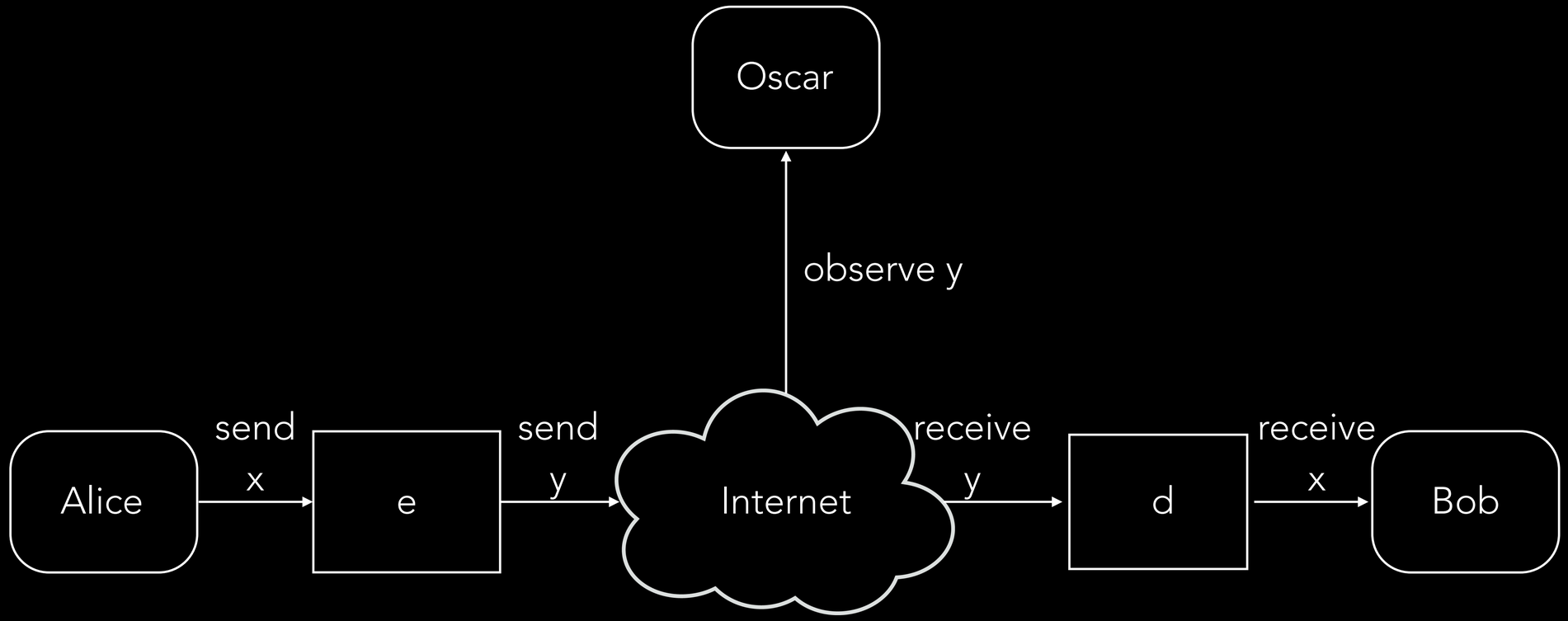
Symmetric-key crypto-system

Data security



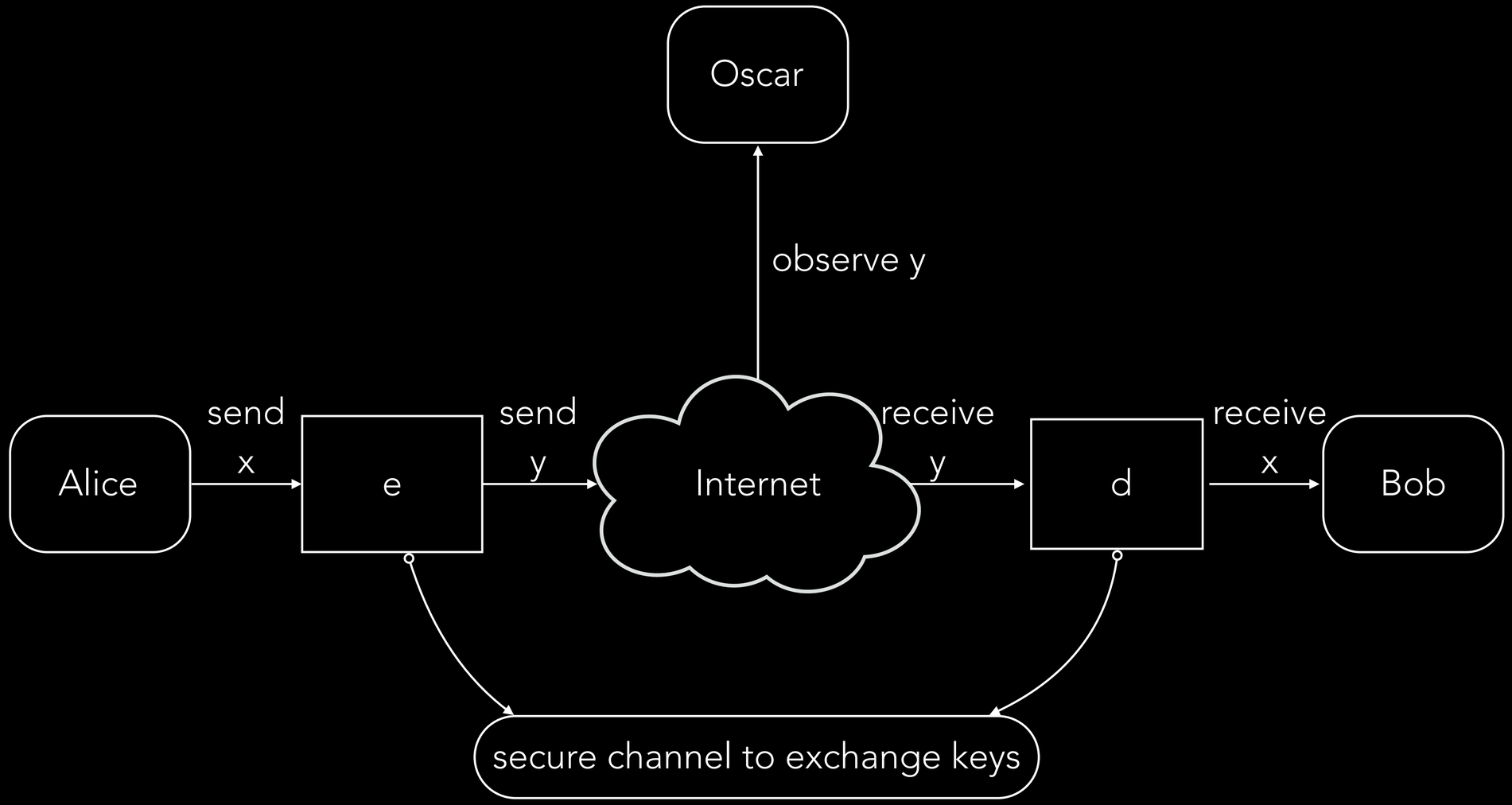
Symmetric-key crypto-system

Data security



Symmetric-key crypto-system

Data security

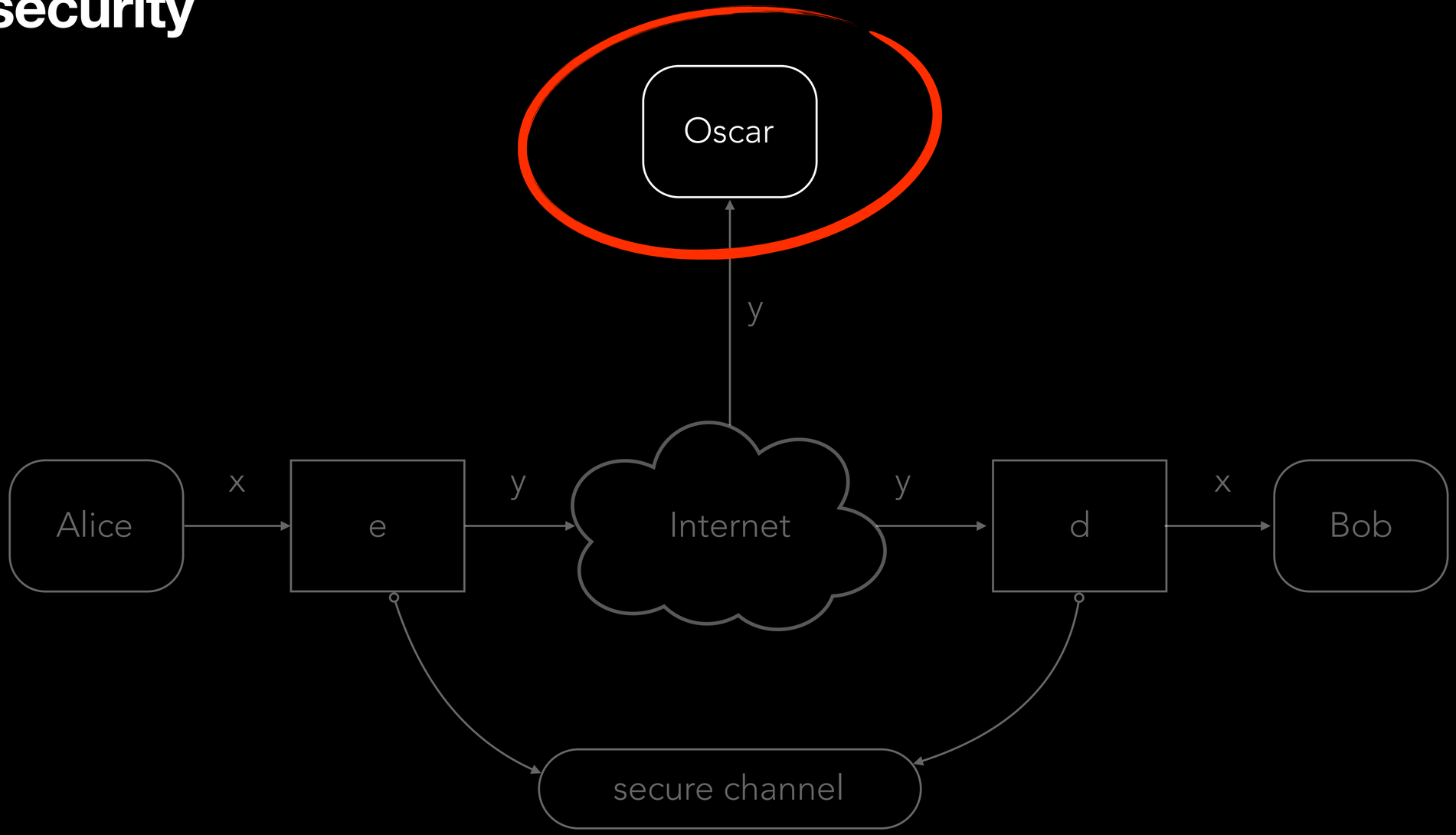


A crypto-system should be secure, even if every aspect of it is public, except the key

Kerckhoffs' Principle

Symmetric-key crypto-system

Data security



Asymmetric-key crypto-system

Asymmetric-key crypto-system

Data security

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

Asymmetric-key crypto-system

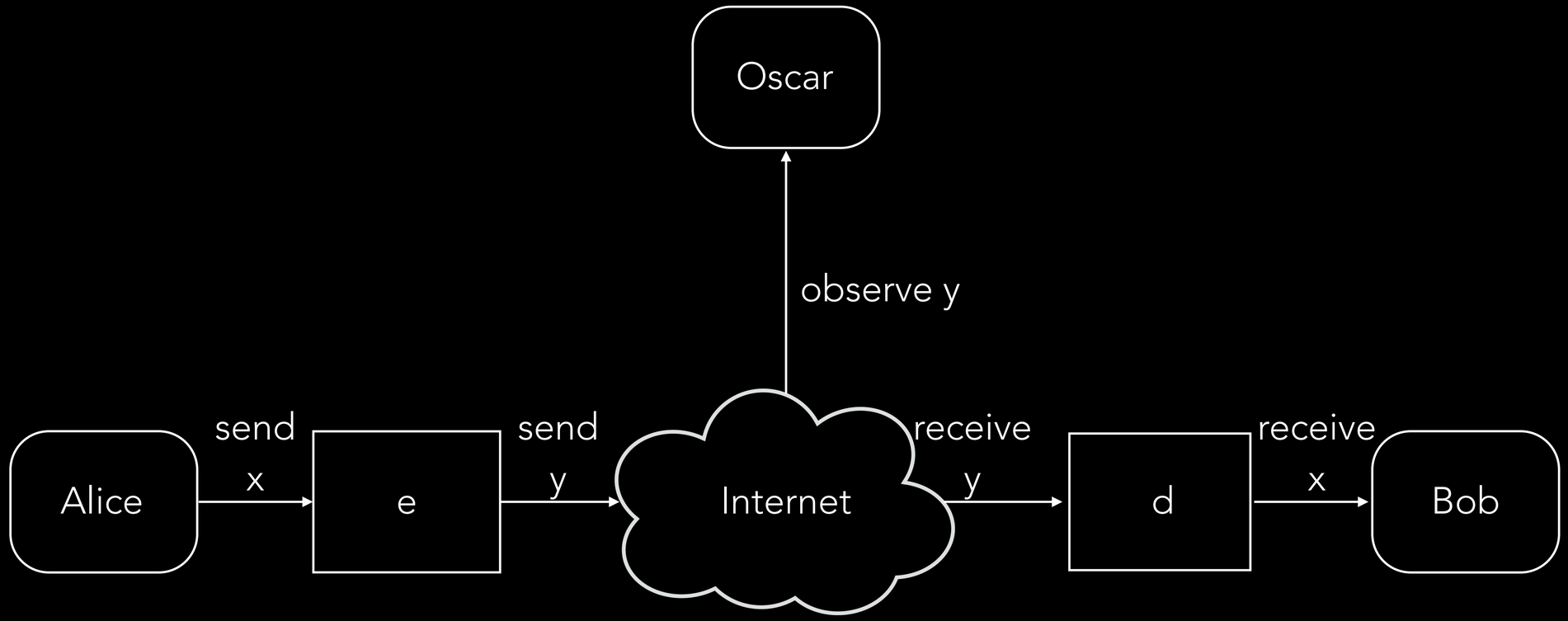
Data security

$$f_{AE}(M, K_{PUBLIC}) = E_D$$

$$f_{AD}(E_D, K_{PRIVATE}) = M$$

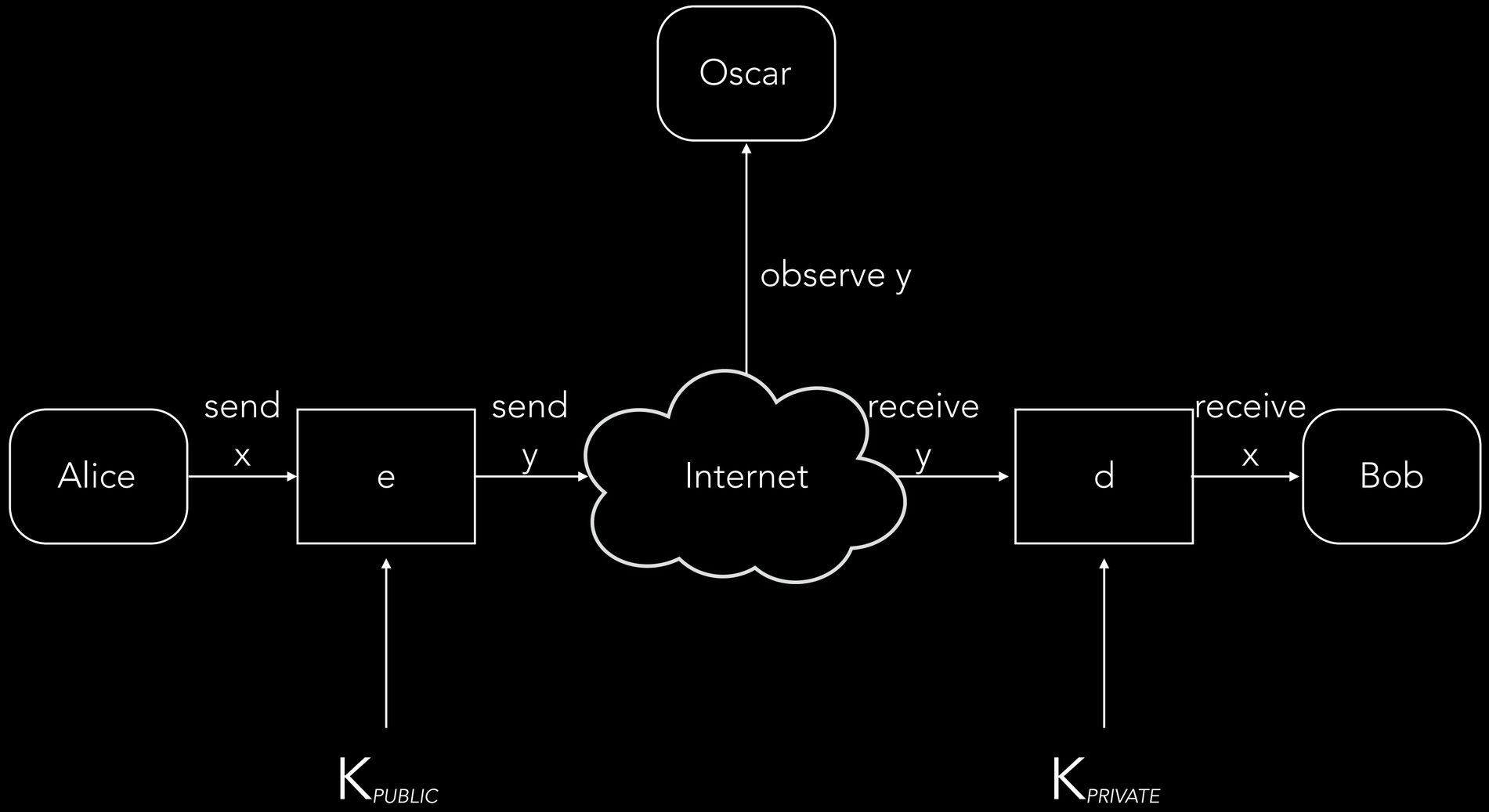
Asymmetric-key crypto-system

Data security



Asymmetric-key crypto-system

Data security



Probabilistic and Deterministic encryption

Data security

Encryption

- Encryption is a process that can be used to ensure the confidentiality of data, ensuring only those that are authorised can consume data.
- The aim of encryption is to readable binary data or **plain text** and use the process to convert the data into a non-readable form or **cipher text**.
- There are many different approaches and strategies to the encryption process and the optimal approach depends on-part on the context.

Probabilistic encryption

Encryption

- Probabilistic encryptions **incorporates randomness into the encryption process**.
- The motivation is that given the same inputs, the **output from the encryption process, generally, will be different**.
- For an encryption process to be considered secure, it **must minimise the level of information leaked about plain text**.
- Probabilistic encryption is an important characteristic to **prevent information leakage** from the plain text, without such a characteristic it may be possible for attackers to determine the original data.

Deterministic encryption

Encryption

- Deterministic encryption **outputs the same cipher text from the same inputs**.
- Deterministic encryption **can not be considered secure** as it effectively leaks information about the plain text or original data.
  - Still secure to some extent and approach can be valuable in other applications.
- The **characteristic is valuable** in delivering approaches that can be used to achieve secure deduplication.

Convergent encryption

Convergent encryption

Encryption

- Convergent encryption is an approach that produces the same output for a given input.
- The approach is sometimes referred to as content hash keying and is viable approach for secure deduplication.
  - Generate fingerprint of the binary data or plain text.
  - Encrypt binary data or plain text using the fingerprint as key.
  - Fingerprint stored, encrypted using user key.

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

$$K = H(M)$$

$$C = E(K, M)$$

Convergent encryption

Encryption

- Using the approach would result in identical cipher texts from different users as the encryption key is the same.
- Consequently, the infrastructure provider can identify duplicated data as the same cipher texts would be produced.
- The encryption key used by individuals is managed and protected by the individual user, so there is no need to become involved in complex key management.

Concerns with convergent encryption

Concerns with convergent encryption

Encryption

- Convergent encryption does not necessarily address concerns of deduplication but can still improve scenario.
- **Confirmation of File** (COF) is in theory in possible by attacker that has the binary data as they can generate the key.
- **Learn-the-remaining-information** (LRI), much like the salary attack, in that the attack already largely knows the binary data but can make small alterations.
- COF and LRI broadly require the attacker to have access to the binary data and the infrastructure.

Convergent Encryption

Business Continuity