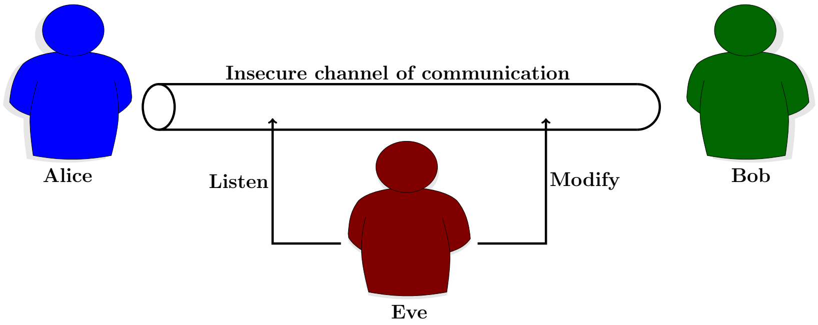
Symmetric Key Cryptography

University of Birmingham

Outline of This Lecture

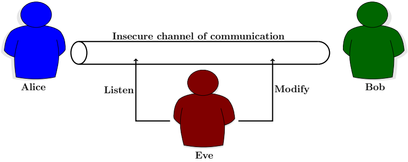
- The framework and the model
- Classical Cryptography and One Time Pad
- Stream Ciphers and Block Ciphers
- Modes of Operations

Setup



Alice and Bob needs to communicate “securely”

Model



- Alice, Bob, and Eve are Algorithms.
- Questions: What is the computation power of Eve?
- Question: What kind of tampering could Eve do?

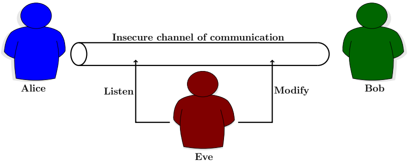
Modelling Eve

- Assume computation power: Million Teraflops $\approx 2^{60}$ computations per second.
- 1 common year= $3600 \times 24 \times 365$ seconds $= 3153600$ seconds $\approx 2^{22}$ seconds.
- Total one year of computation $\approx 2^{82}$ computations

Modelling Eve

- Assume computation power: Million Teraflops $\approx 2^{60}$ computations per second.
- 1 common year= $3600 \times 24 \times 365$ seconds $= 3153600$ seconds $\approx 2^{22}$ seconds.
- Total one year of computation $\approx 2^{82}$ computations
- Ballpark estimate of Eve's power $\approx 2^{100}$ computations: accepted standard for non-classified data.

Model



- Alice, Bob, and Eve are Algorithms.
- Questions: What is the computation power of Eve? 2^{100} computations.
- Question: What kind of tampering could Eve do?

Modelling Eve: Channel Modification

- Could Eve erase everything? If yes, no communication could be done.

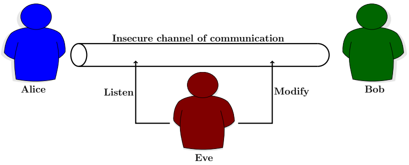
Modelling Eve: Channel Modification

- Could Eve erase everything? If yes, no communication could be done.
- Could Eve modify small fraction of data (say 1/4)?
  - We use error correcting codes to correct errors. (beyond the scope)

Modelling Eve: Channel Modification

- Could Eve erase everything? If yes, no communication could be done.
- Could Eve modify small fraction of data (say 1/4)?
    - We use error correcting codes to correct errors. (beyond the scope)
- Cryptographic modeling: Eve could modify *any* fraction, we care about *error detection*.

Model



- Alice, Bob, and Eve are Algorithms.
- Computation power of Eve? 2^{100} for non-classified data
- Eve could modify any part: Alice and Bob need error detection.

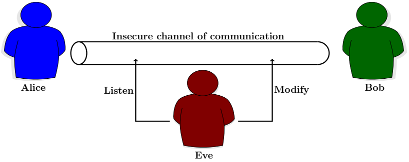
Question

What does Eve know?

Kerckhoffs's principle: Second Rule

- System should not require secrecy. Algorithms of Alice and Bob are public information.

Model

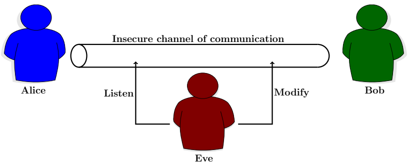


- Alice, Bob, and Eve are Algorithms.
- Computation power of Eve? 2^{100} for non-classified data
- Eve could modify any part: Alice and Bob need error detection.

Question

What does Eve know? Alice and Bob's algorithms.

Model



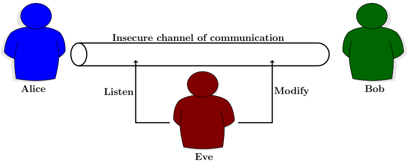
- Alice, Bob, and Eve are Algorithms.
- Computation power of Eve? 2^{100} for non-classified data
- Eve could modify any part: Alice and Bob need error detection.

Question

What does Eve know? Alice and Bob's algorithms.

No Secrecy Yet: Eve could run Bob's algorithm on the communication!

Model: the KEY to secure communication



- Alice, Bob, and Eve are Algorithms.
- Computation power of Eve? 2^{100} for non-classified data
- Eve could modify any part: Alice and Bob need error detection.

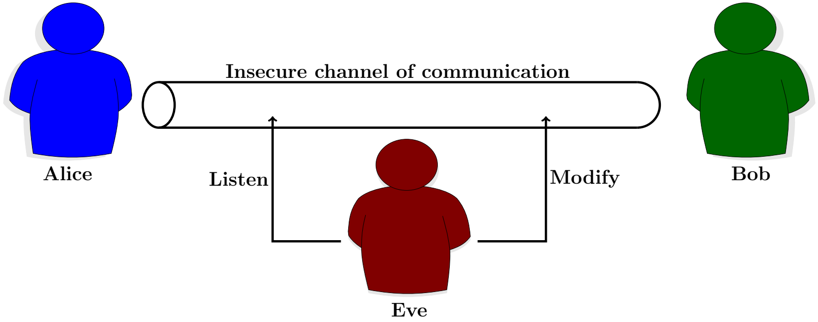
Question

What does Eve know? Alice and Bob's algorithms.

secret key

A secret information known to Bob; unknown to Eve.

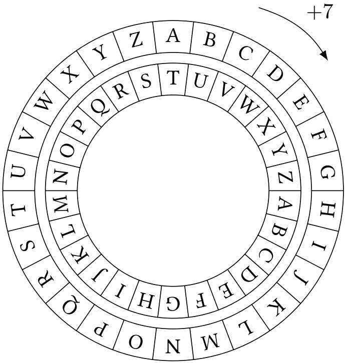
Symmetric Key Cryptography



Setup in symmetric key cryptography

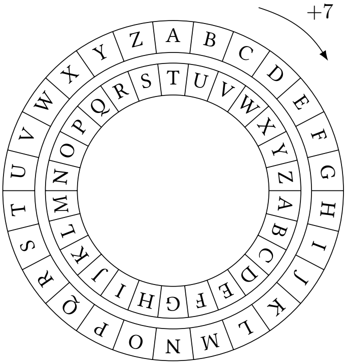
Alice and Bob <u>both</u> know the secret key. Eve does not know the secret key.

Symmetric Key Cryptography: Historic account



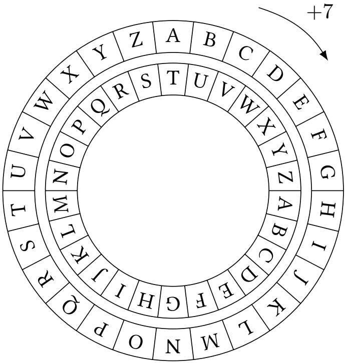
- SECURITY $\rightarrow$ ZLJBYPAF

Symmetric Key Cryptography: Historic account



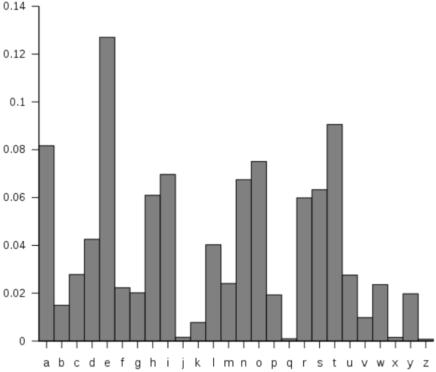
- SECURITY $\rightarrow$ ZLJBYPAF
- Decryption requires going back 7 characters

Symmetric Key Cryptography: Historic account



- SECURITY $\rightarrow$ ZLJBYPAF
- Decryption requires going back 7 characters
- Could be generalised to any number between 1 to 26. The number is going to be the key.

Ceaser Cipher: Cryptanalysis



- Broken using frequency analysis: 'e' is the most frequent character, followed by 't' then 'a'
- for sufficiently long ciphertext, shift by fixed length maintains the relative frequency.
  - For $+7$ shift, 'l' is most frequent, followed by 'a' and 'h'

One Time Pad

- For each character a random shift is chosen.
- the sequence of shift (number) is the key

Plain text: T H I S I S S E C R E T
OTP-Key : X V H E U W N O P G D Z

Ciphertext: Q C P W C O F S R X H S
In groups : QCPWC OFSRX HS

- Perfect Secrecy when the key is random.

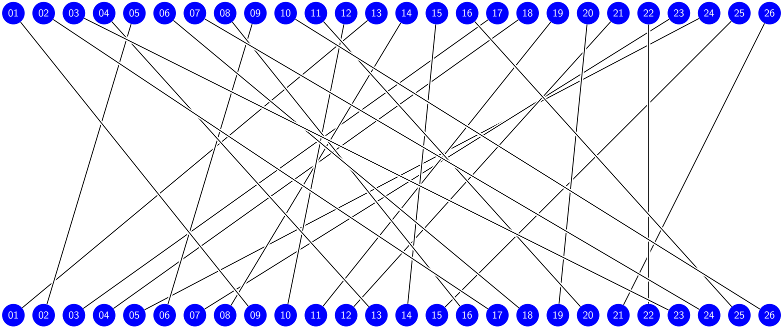
Issues with one time pad

- Key has to be as long as the text.
- Can not repeat key.

Encrypting with Smaller Keys

- **Block Cipher** Encrypt n-bit block via a randomly chosen permutation.
- **Stream Cipher** Generate a *random looking* bit-stream from a smaller key and xor the message with the stream

Encryptions are Permutations



Block Ciphers

- Message Space $\mathcal{M}$, typically $\{0,1\}^{128}$

Number of possible Permutations

factorial (2^{128})

Block Ciphers

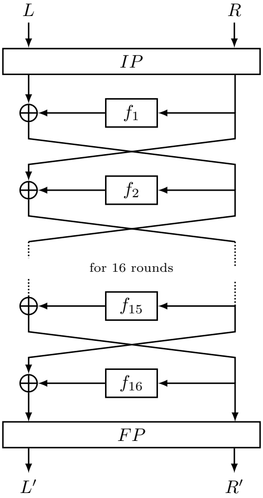
- Message Space $\mathcal{M}$, typically $\{0,1\}^{128}$
- Key Space $\mathcal{K}$, say $\{0,1\}^{128}$

Number of possible Permutations

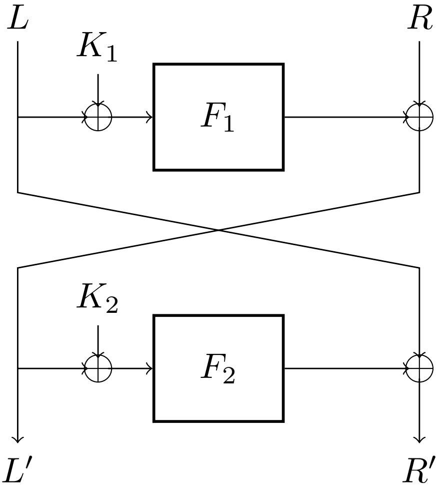
factorial (2^{128})

A block cipher over the keyspace $\{0,1\}^{128}$ is a family of 2^{128} many permutations

Block Cipher Designs:DES



Design Principle: Feistel Network



Block Cipher Designs:AES

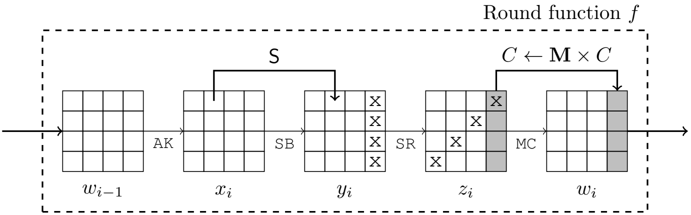
$\mathcal{M} = \{0,1\}^{128}$. Each domain element is 16-bytes long.

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Block Cipher Designs:AES

$\mathcal{M} = \{0,1\}^{128}$. Each domain element is 16-bytes long.

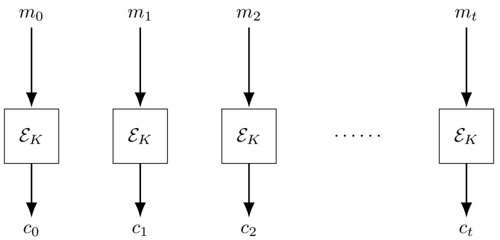
0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15



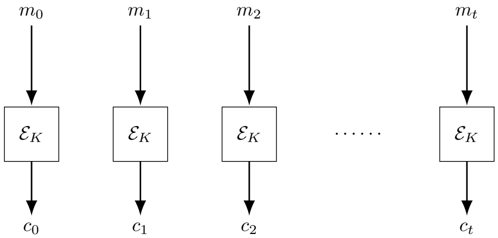
Modes of Operations

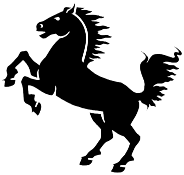
- Block ciphers encrypt fixed length strings: AES encrypts 128 bits.
- How to encrypt large messages? Modes of operations

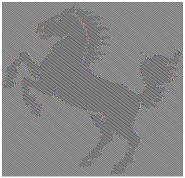
Electronic Code Book: Parallel applications of block cipher



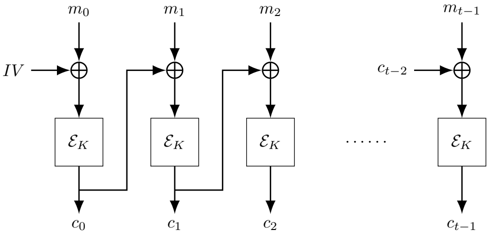
Electronic Code Book: Parallel applications of block cipher







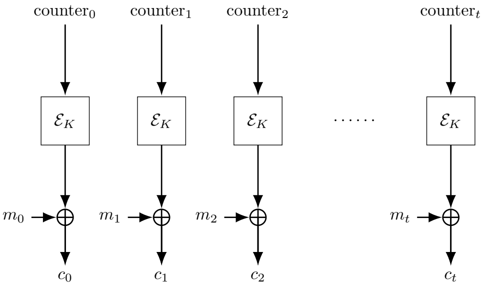
CBC mode



Caution

IV needs to be random!

Counter mode



Caution

Ciphertexts are malleable.