

Code-Based Cryptography

Error-Correcting Codes and Cryptography

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. **Introduction II - Coding Theory**
3. Encoding (Linear Transformation)
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. McEliece Cryptosystem

Introduction to Coding Theory

“A Mathematical Theory of Communication”
(Claude Shannon, 1948)

Introduction to Coding Theory

"A Mathematical Theory of Communication"
(Claude Shannon, 1948)

```
graph TD; A["A Mathematical Theory of Communication (Claude Shannon, 1948)"] --> B["Coding Theory"]; A --> C["Information Theory"];
```

The diagram illustrates the foundational role of Claude Shannon's 1948 paper, "A Mathematical Theory of Communication," in the development of Coding Theory and Information Theory. A central grey box at the top contains the title and author of the paper. Two curved arrows point from this box to two separate red boxes below it, labeled "Coding Theory" and "Information Theory," indicating that the paper's work is the basis for both fields.

Coding Theory

Information Theory

Introduction to Coding Theory

"A Mathematical Theory of Communication"
(Claude Shannon, 1948)

```
graph TD; A["A Mathematical Theory of Communication (Claude Shannon, 1948)"] --> B["Coding Theory"]; A --> C["Information Theory"];
```

The diagram illustrates the foundational role of Claude Shannon's 1948 paper, "A Mathematical Theory of Communication," in the development of Coding Theory and Information Theory. A central grey box at the top contains the title and author. Two curved arrows point from this box to two separate red boxes below, labeled "Coding Theory" and "Information Theory," indicating that the paper's work underpins both fields.

Coding Theory

Information Theory

"Efficient transfer reliable information"

Communication System

Alphabet: $\mathcal{A}$



Communication System

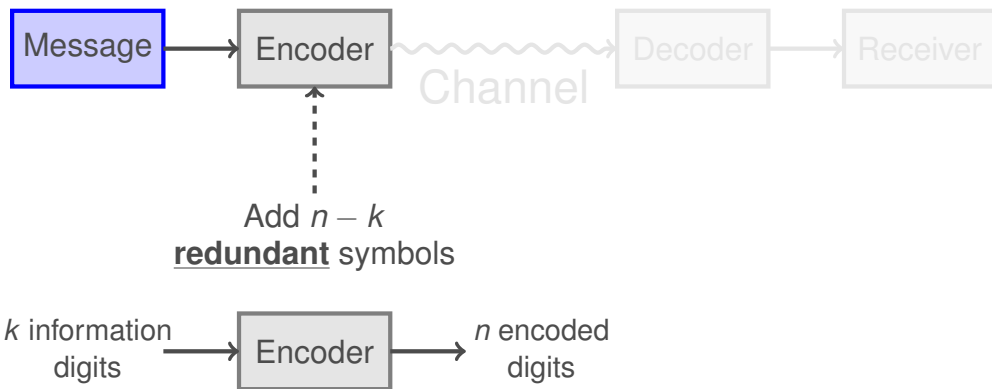
Alphabet: $\mathcal{A}$



$$\mathbf{m} = (m_1 \dots, m_k) \in \mathcal{A}^k$$

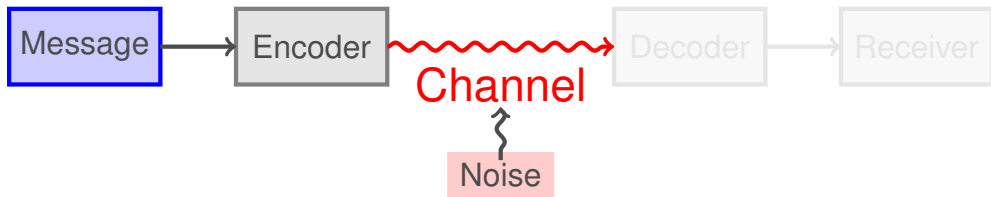
Communication System

Alphabet: $\mathcal{A}$



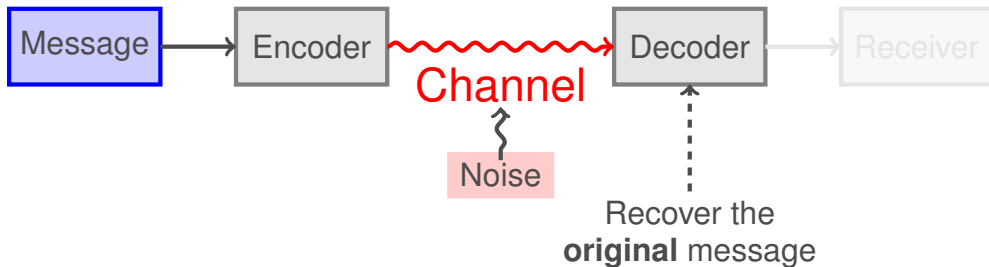
Communication System

Alphabet: $\mathcal{A}$



Communication System

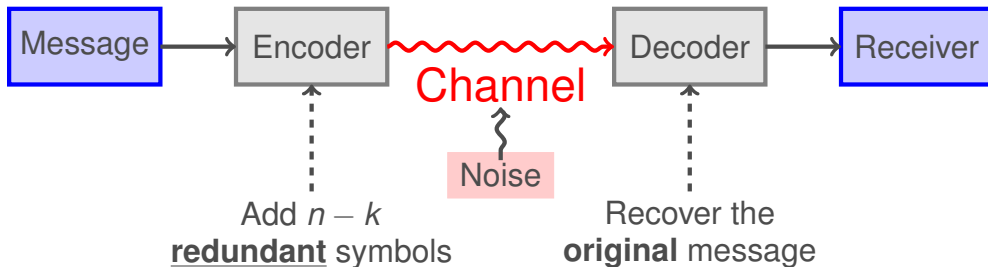
Alphabet: $\mathcal{A}$



$$\text{Decoder} \left(\underbrace{\text{Encoder} (\text{Message})}_{\text{codeword}} + \text{Noise} \right) = \text{Message}$$

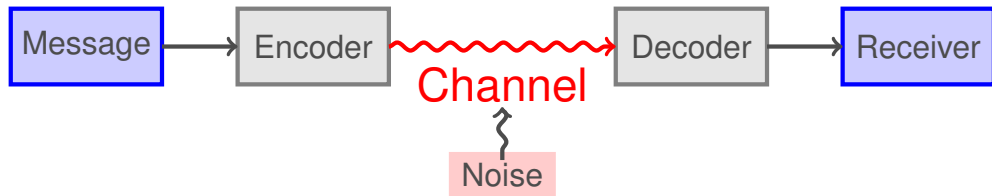
Communication System

Alphabet: $\mathcal{A}$



$$\text{Decoder} \left(\underbrace{\text{Encoder} (\text{Message})}_{\text{codeword}} + \text{Noise} \right) = \text{Message}$$

Communication System - Repetition code



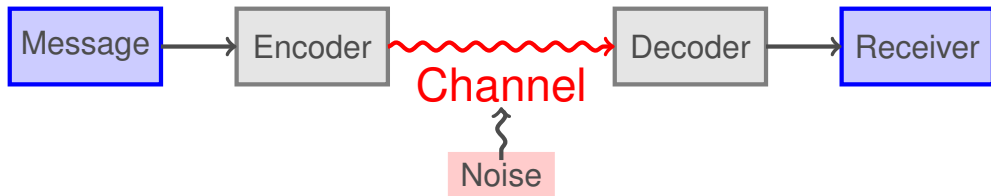
1. **Alphabet:** $\mathcal{A}$ = English Alphabet

Yes

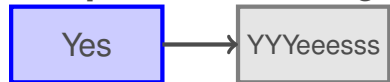
2. **Alphabet:** $\mathcal{A} = \mathbb{F}_2$

1

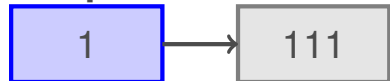
Communication System - Repetition code



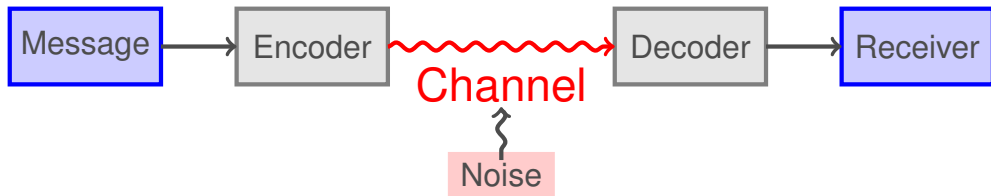
1. **Alphabet:** $\mathcal{A}$ = English Alphabet



2. **Alphabet:** $\mathcal{A} = \mathbb{F}_2$



Communication System - Repetition code



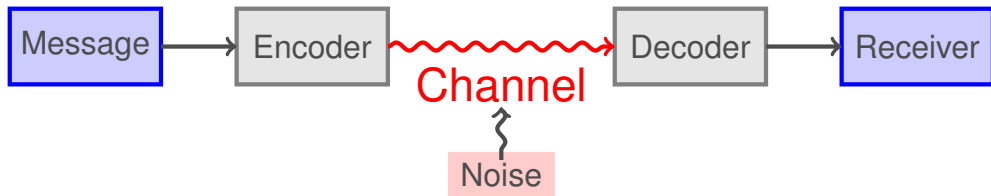
1. **Alphabet:** $\mathcal{A}$ = English Alphabet



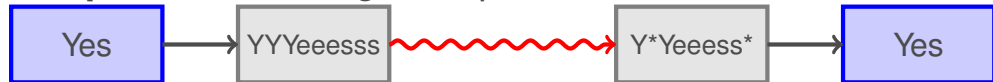
2. **Alphabet:** $\mathcal{A} = \mathbb{F}_2$



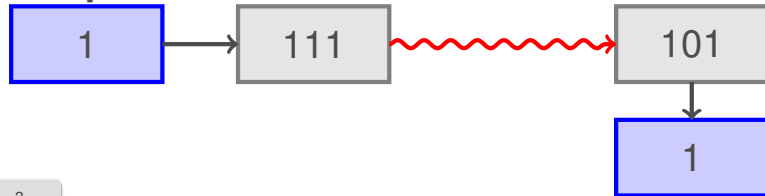
Communication System - Repetition code



1. **Alphabet:** $\mathcal{A}$ = English Alphabet



2. **Alphabet:** $\mathcal{A} = \mathbb{F}_2$



Claude Shannon



Claude Shannon



→ Definition of Information

Claude Shannon



- Definition of Information
- “Channel Coding Theorems”

Claude Shannon



→ Definition of Information

→ “Channel Coding Theorems”

“For any communication channel it is possible to communicate discrete data nearly error free up to a maximum rate (**channel capacity**)”

Check Digit

A **check digit** is a redundancy bit used for detecting one error

Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:

Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:

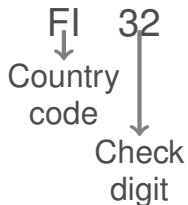
FI
↓
Country
code

Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:

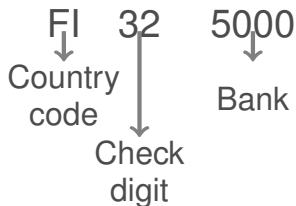


Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:

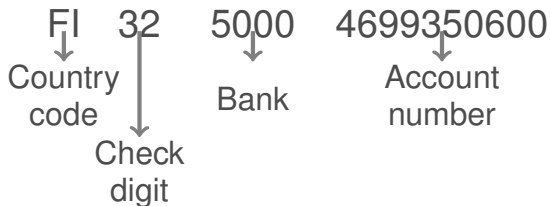


Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:

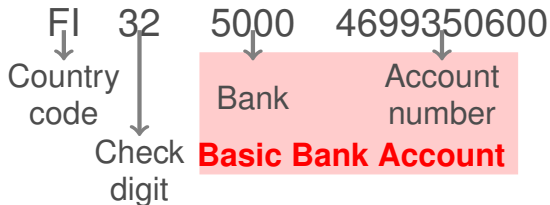


Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:

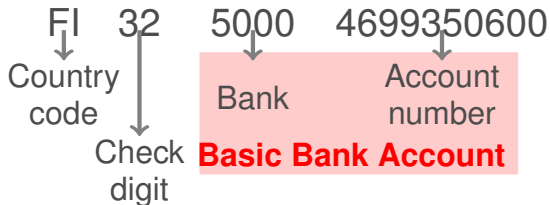


Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:



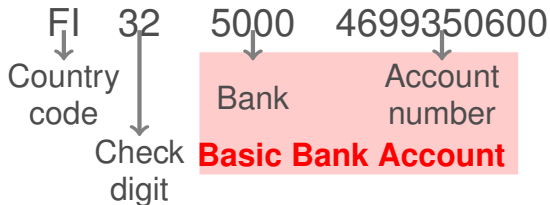
FI32 5000 4699350600

Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:



32 5000 4699350600 FI

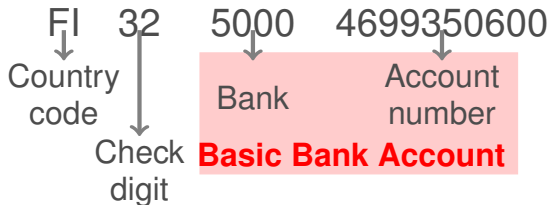
1. Rearrange

Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:



32 5000 4699350600 **1518**

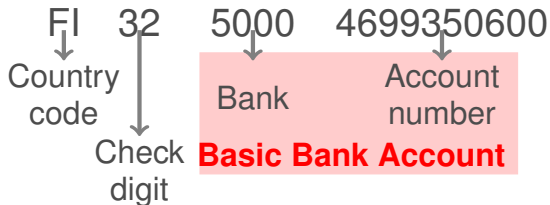
1. Rearrange
2. Convert to Integer

Check Digit

A **check digit** is a redundancy bit used for detecting one error

International Bank Account Number (IBAN)

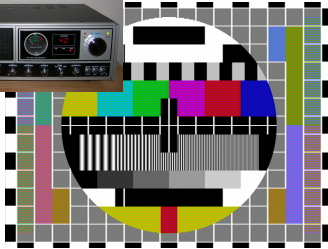
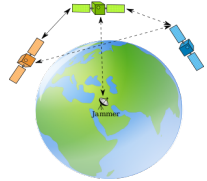
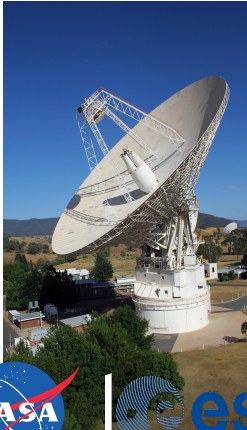
The **IBAN** is used for identifying bank account across national borders.
It consist of 4 elements:



$$32\ 5000\ 4699350600\mathbf{1518} \equiv 1 \pmod{97}$$

1. Rearrange
2. Convert to Integer
3. Validate

Error correcting codes in our daily life



Coding Theory vs. Cryptography

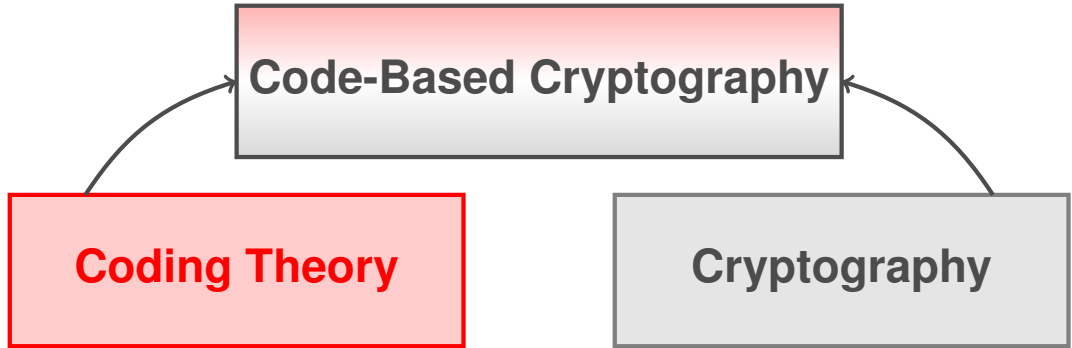
Coding Theory

Coding Theory vs. Cryptography

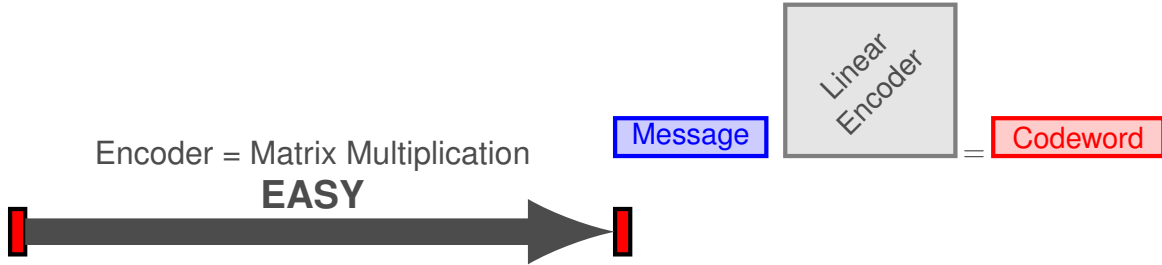
Coding Theory

Cryptography

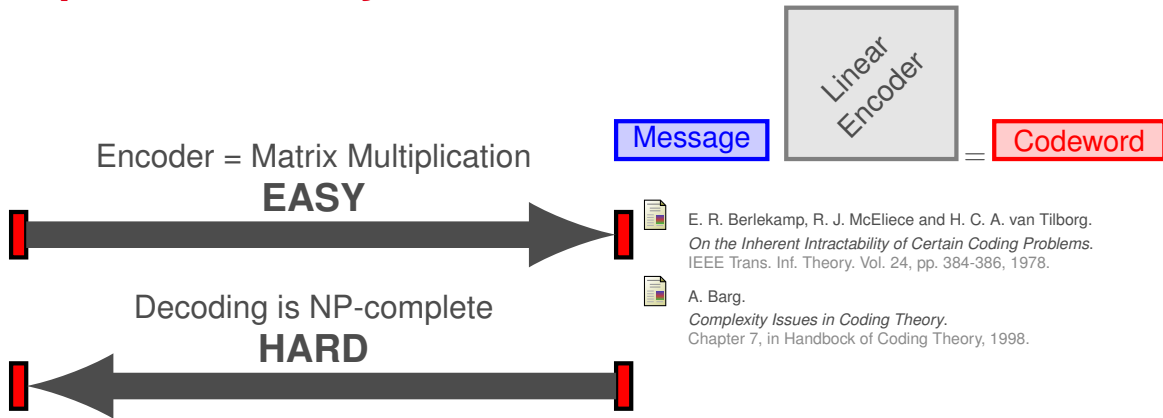
Coding Theory vs. Cryptography



Trapdoor one-way functions - Decoder



Trapdoor one-way functions - Decoder



Trapdoor one-way functions - Decoder

Encoder = Matrix Multiplication

EASY

Message

Linear
Encoder

Codeword

Decoding is NP-complete

HARD

Efficient decoder for certain families of codes

EASY (with TRAPDOOR information)

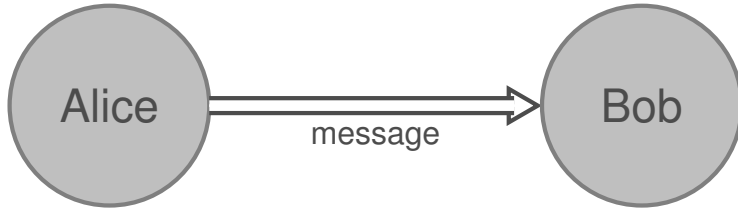


E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg.
On the Inherent Intractability of Certain Coding Problems.
IEEE Trans. Inf. Theory. Vol. 24, pp. 384-386, 1978.



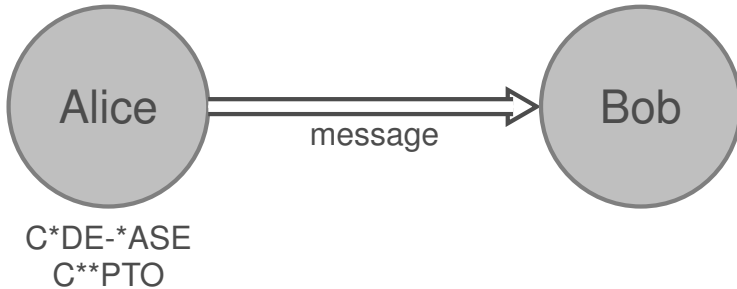
A. Barg.
Complexity Issues in Coding Theory.
Chapter 7, in Handbook of Coding Theory, 1998.

How to use Coding Theory in Cryptography?



How to use Coding Theory in Cryptography?

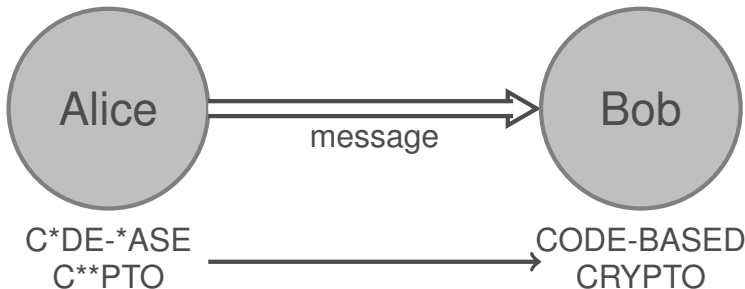
Adds errors
in the message



How to use Coding Theory in Cryptography?

Adds errors
in the message

Knows an efficient
decoding method



1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. **Encoding (Linear Transformation)**
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. McEliece Cryptosystem

Pictures Licenses

- p. 4: Claude Shannon / This image is used courtesy of MIT Museum - more images available at: [MIT Museum Collections - People](#).
- p. 6: Rights Reserved