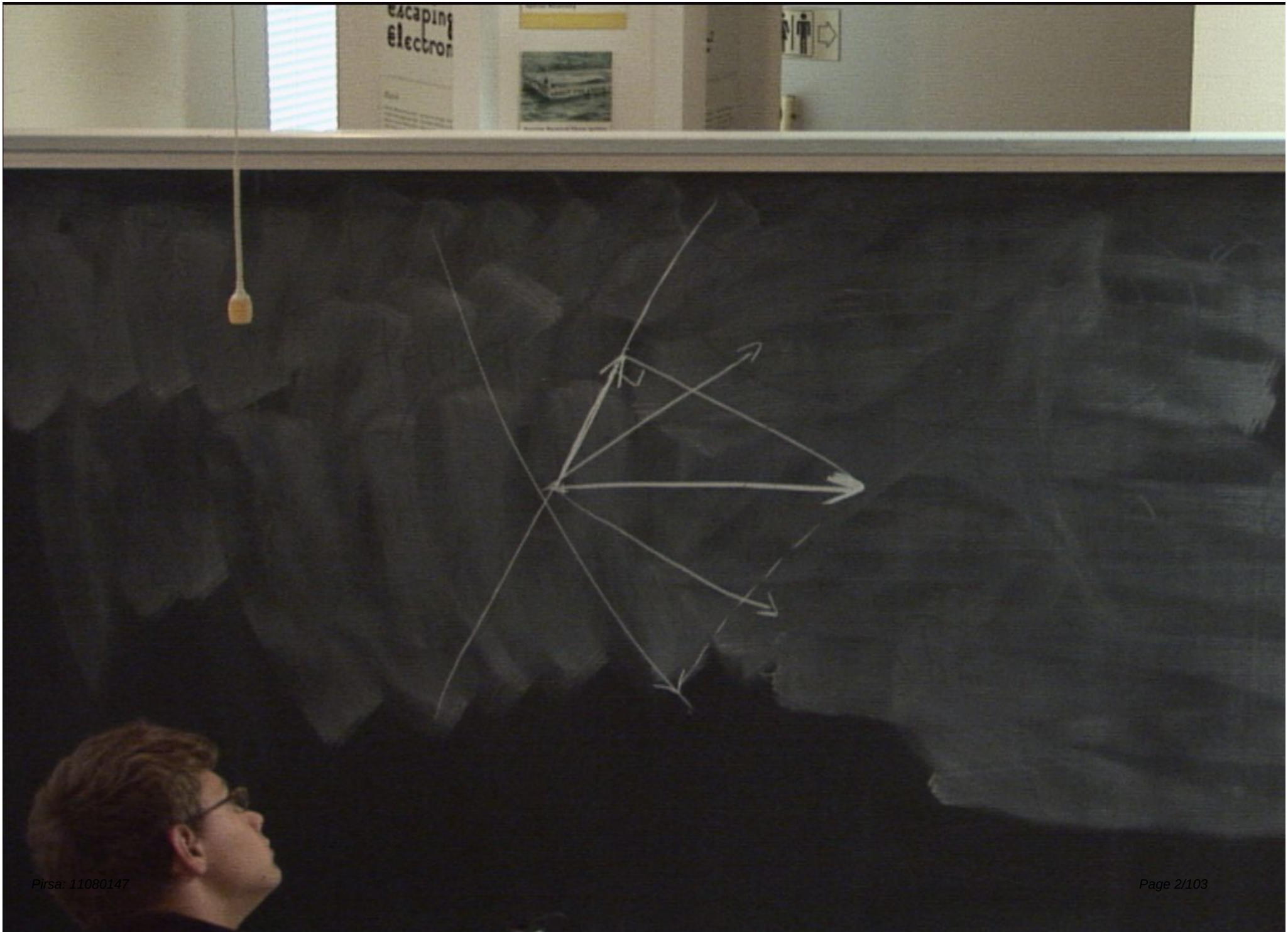
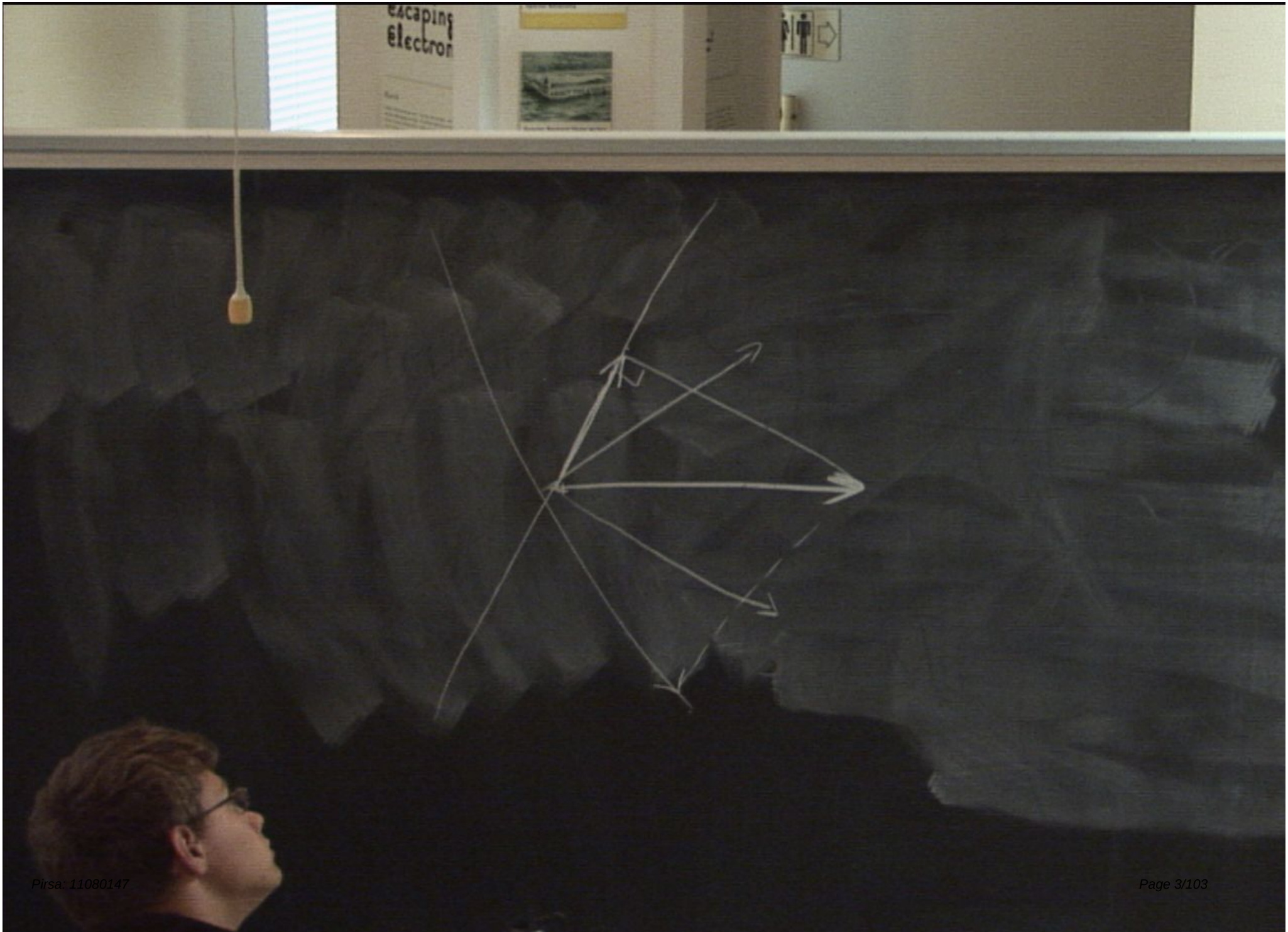
Title: ISSYP 2011 - Quantum Cryptograpy

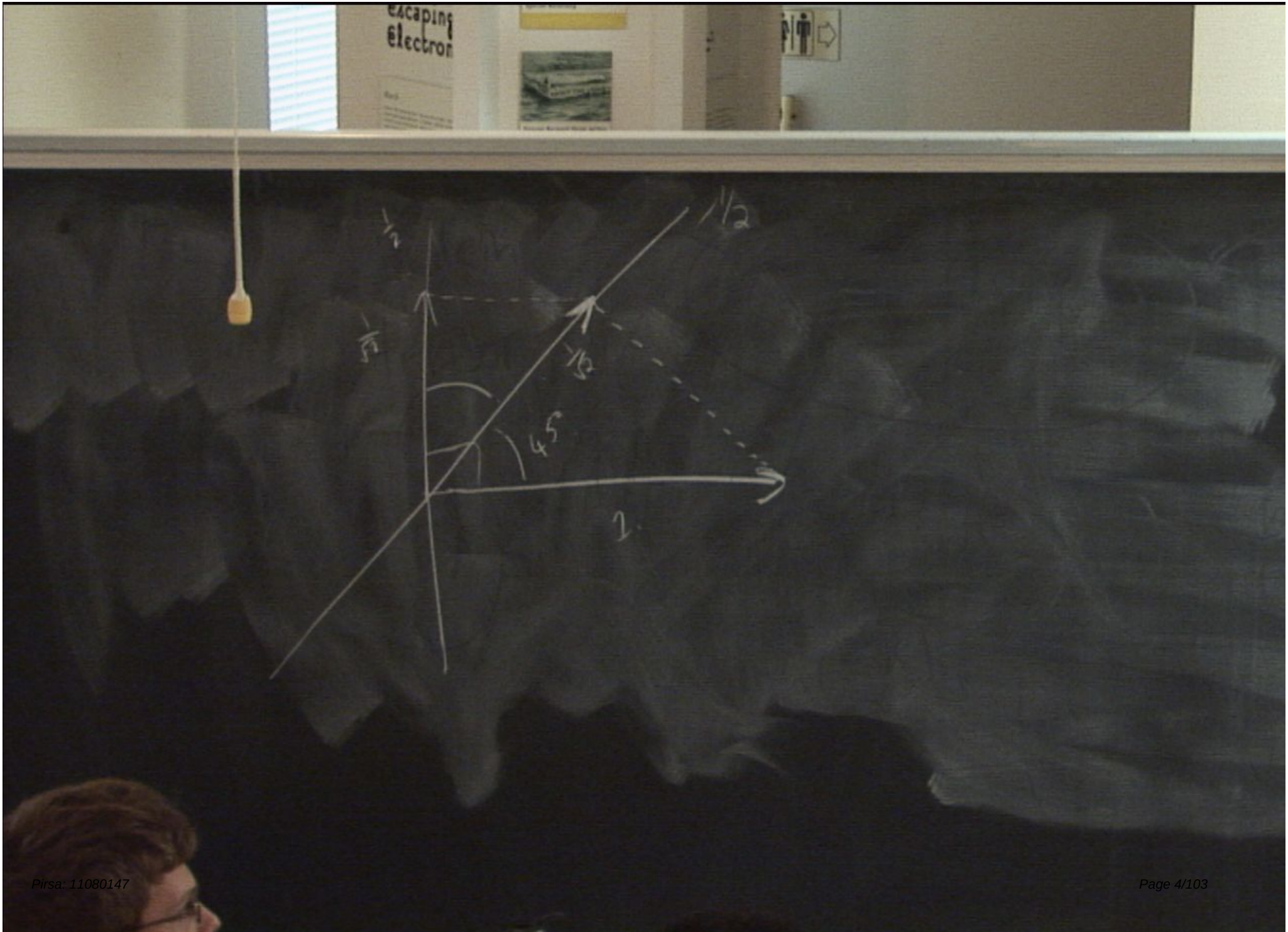
Date: Aug 03, 2011 10:30 AM

URL: http://pirsa.org/11080147

Abstract: This is an introductory talk on quantum cryptography, focusing on quantum key distribution (QKD) with a cool little demo involving polarized light. QKD gives us the amazing ability to send messages with absolute security


escaping
electron


Escaping
Electron


escaping
electron
1/2
1/2
1/√2
1/√2
45
1.

Polarization of light

Polarization of light

- Diagonal = horizontal + vertical

Polarization of light

- Diagonal = horizontal + vertical

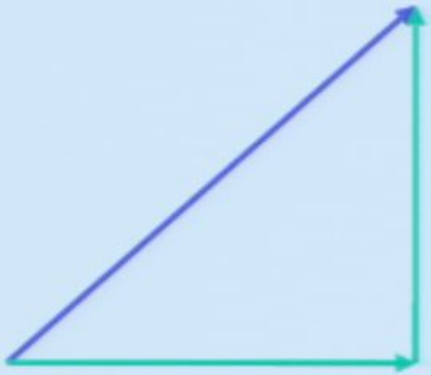
Polarization of light

- Diagonal = horizontal + vertical

- Horizontal component of light passes through; Vertically polarized component is blocked

Polarization of light

- Diagonal = horizontal + vertical



- Horizontal component of light passes through; Vertically polarized component is blocked
- Not a bulk phenomenon

Spot the difference?

Spot the difference?

- Which photo was taken with a polarizing filter?

Spot the difference?

- Which photo was taken with a polarizing filter?
- Light reflected from the windows is polarized
- The filter absorbs the polarized light

Encryption

- Alice wants to send a note to Bob across the room
- Passes it to a neighbour, to be passed on to Bob
- How can she keep the others from reading the contents?

Caeser cipher

Caeser cipher

- Earliest recorded method known
- Substitute letters by other letters, e.g., shift by 3

Caeser cipher

- Earliest recorded method known
- Substitute letters by other letters, e.g., shift by 3

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

Caeser cipher

- Earliest recorded method known
- Substitute letters by other letters, e.g., shift by 3

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

- Example

```
the quick brown fox jumps over the lazy dog
```

Caeser cipher

- Earliest recorded method known
- Substitute letters by other letters, e.g., shift by 3

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

- Example

```
the quick brown fox jumps over the lazy dog
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
```

How secure is this?

How secure is this?

- Shifts are easy to break: try all shifts

How secure is this?

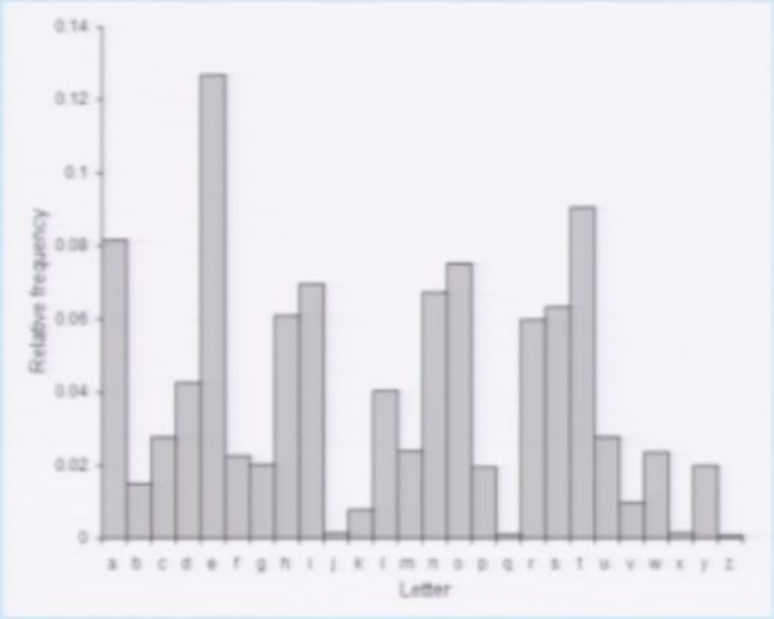
- Shifts are easy to break: try all shifts
- Other single letter substitution ciphers?

How secure is this?

- Shifts are easy to break: try all shifts
- Other single letter substitution ciphers?
- Many permutations of the alphabet (26!)

Substitution ciphers

- Frequency analysis known as early as 9th century AD



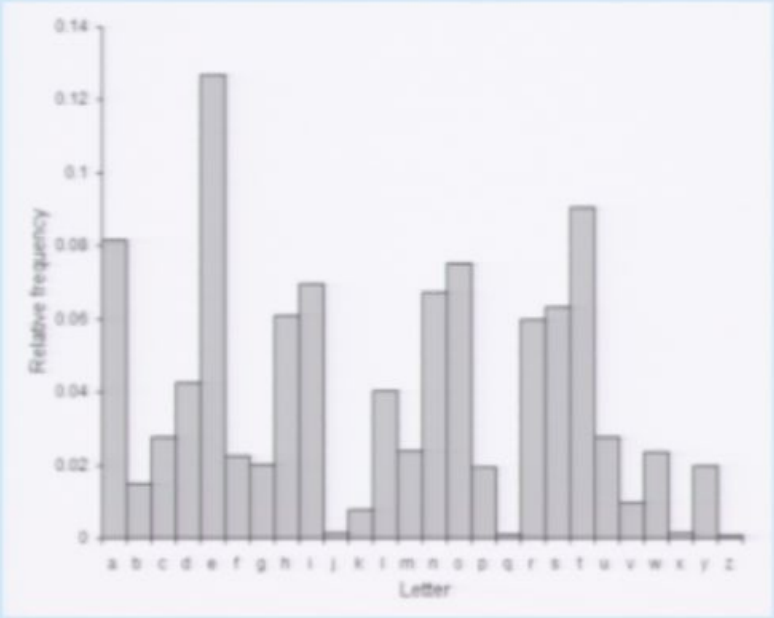
- Compare frequency of letters in ciphertext with that in typical text

How secure is this?

- Shifts are easy to break: try all shifts
- Other single letter substitution ciphers?
- Many permutations of the alphabet (26!)

Substitution ciphers

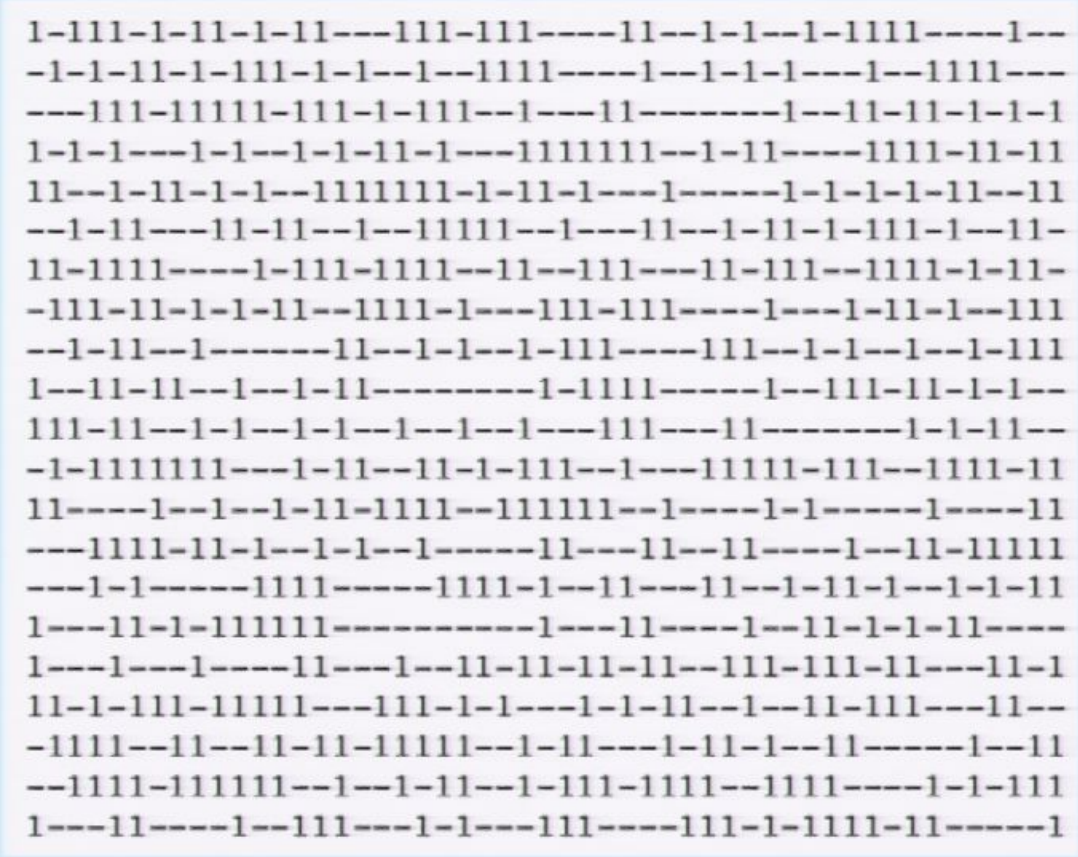
- Frequency analysis known as early as 9th century AD



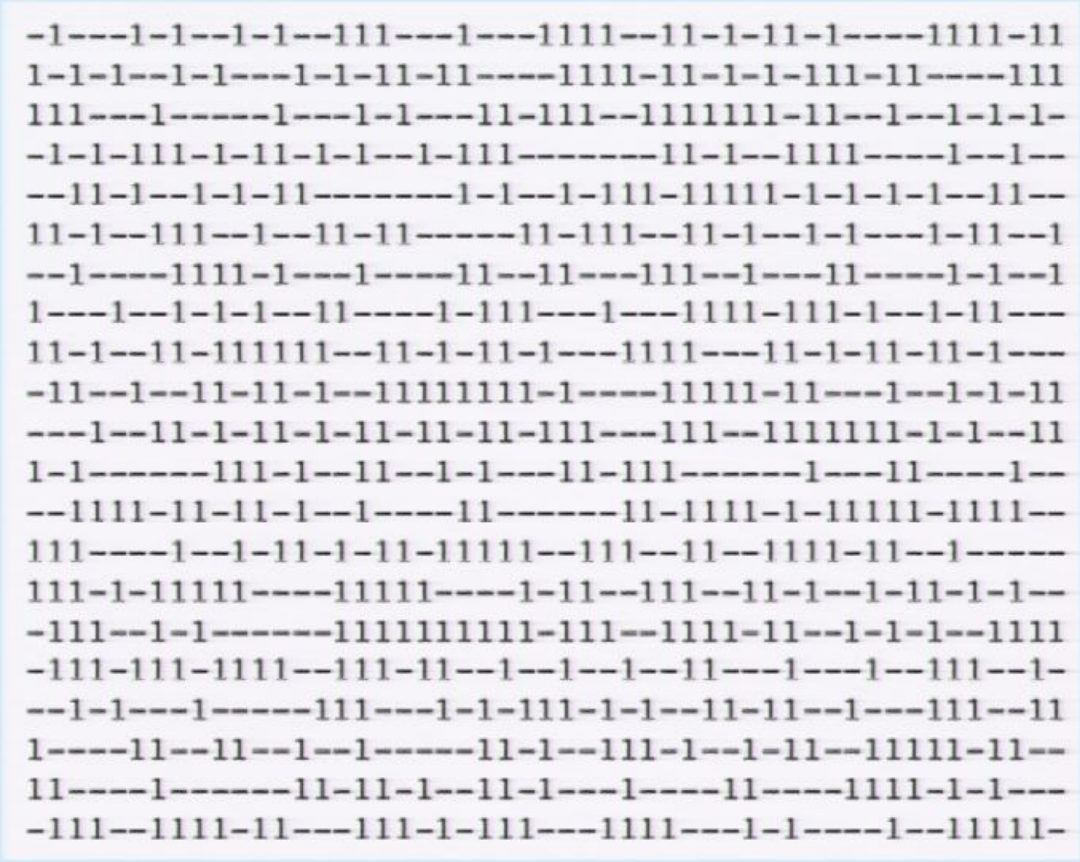
- Compare frequency of letters in ciphertext with that in typical text

Spot the “difference”

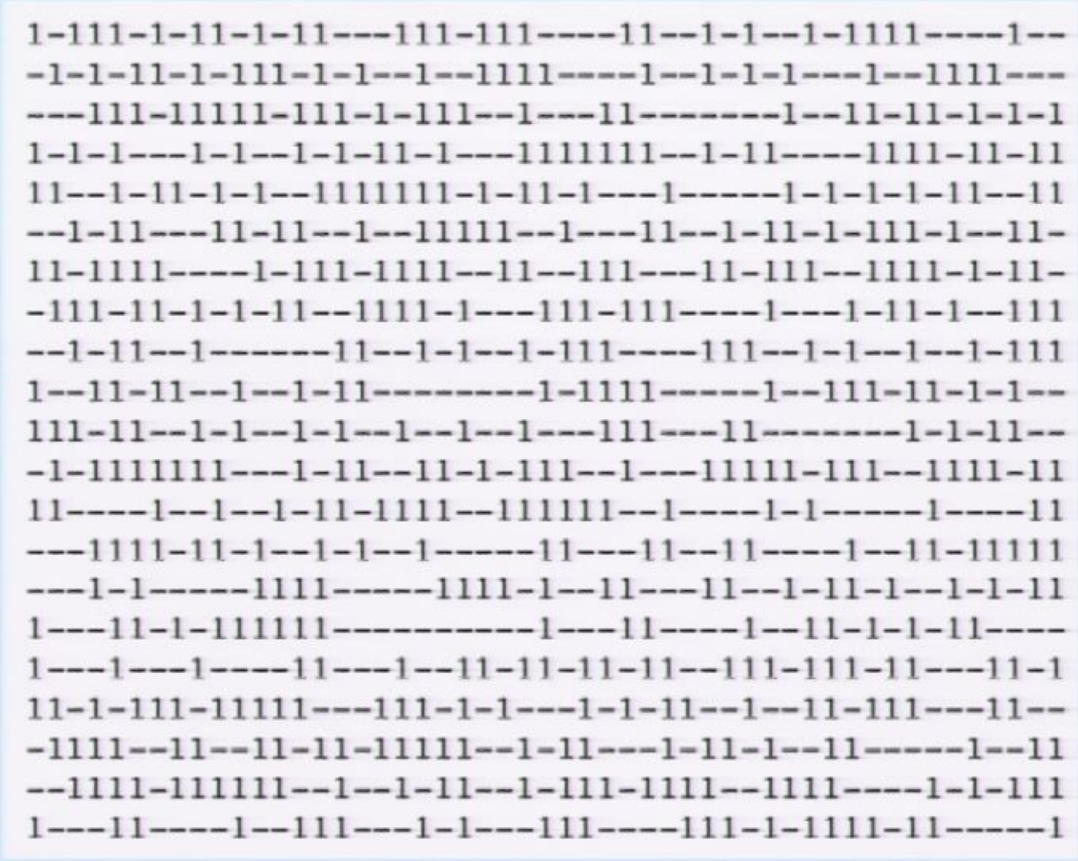
Text A


1-111-1-11-1-11---111-111----11--1-1--1-1111----1--
-1-1-11-1-111-1-1--1--1111----1--1-1-1---1--1111---
---111-11111-111-1-111--1---11-------1--11-11-1-1-1
1-1-1---1-1--1-1-11-1---1111111--1-11----1111-11-11
11--1-11-1-1--1111111-1-11-1---1-----1-1-1-1-11--11
--1-11---11-11--1--11111--1---11--1-11-1-111-1--11-
11-1111----1-111-1111--11--111---11-111--1111-1-11-
-111-11-1-1-11--1111-1---111-111----1---1-11-1--111
--1-11--1------11--1-1--1-111----111--1-1--1--1-111
1--11-11--1--1-11--------1-1111-----1--111-11-1-1--
111-11--1-1--1-1--1--1--1---111---11-------1-1-11--
-1-1111111---1-11--11-1-111--1---11111-111--1111-11
11----1--1--1-11-1111--111111--1----1-1-----1----11
---1111-11-1--1-1--1-----11---11--11----1--11-11111
---1-1-----1111-----1111-1--11---11--1-11-1--1-1-11
1---11-1-111111----------1---11----1--11-1-1-11----
1---1---1----11---1--11-11-11-11--111-111-11---11-1
11-1-111-11111---111-1-1---1-1-11--1--11-111---11--
-1111--11--11-11-11111--1-11---1-11-1--11-----1--11
--1111-111111--1--1-11--1-111-1111--1111----1-1-111
1---11----1--111---1-1---111----111-1-1111-11-----1

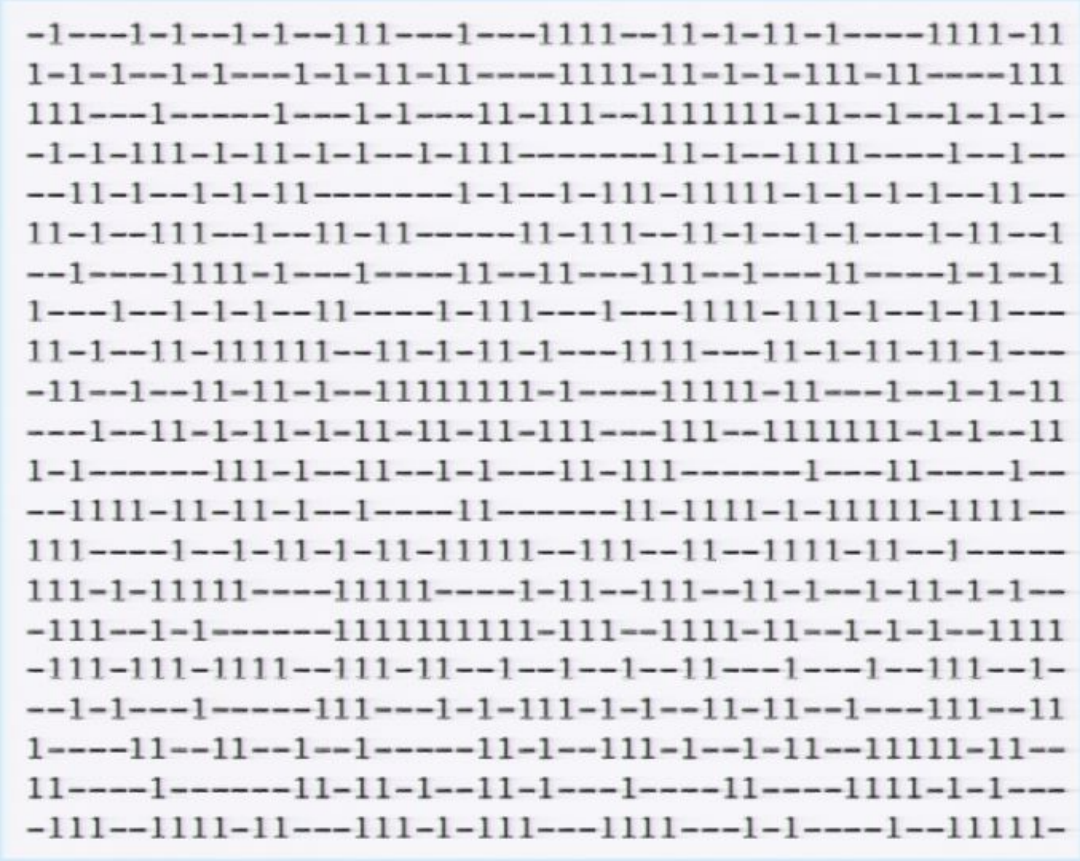
Text B


-1---1-1--1-1--111---1---1111--11-1-11-1----1111-11
1-1-1--1-1---1-1-11-11----1111-11-1-1-111-11----111
111---1-----1---1-1---11-111--1111111-11--1--1-1-1-
-1-1-111-1-11-1-1--1-111-------11-1--1111----1--1--
--11-1--1-1-11-------1-1--1-111-11111-1-1-1-1--11--
11-1--111--1--11-11-----11-111--11-1--1-1---1-11--1
--1----1111-1---1----11--11---111--1---11----1-1--1
1---1--1-1-1--11----1-111---1---1111-111-1--1-11---
11-1--11-111111--11-1-11-1---1111---11-1-11-11-1---
-11--1--11-11-1--11111111-1----11111-11---1--1-1-11
---1--11-1-11-1-11-11-11-111---111--1111111-1-1--11
1-1-----111-1--11--1-1---11-111------1---11----1--
--1111-11-11-1--1----11------11-1111-1-11111-1111--
111----1--1-11-1-11-11111--111--11--1111-11--1-----
111-1-11111----11111----1-11--111--11-1--1-11-1-1--
-111--1-1------1111111111-111--1111-11--1-1-1--1111
-111-111-1111--111-11--1--1--1--11---1---1--111--1-
--1-1---1-----111---1-1-111-1-1--11-11--1---111--11
1----11--11--1--1-----11-1--111-1--1-11--11111-11--
11----1------11-11-1--11-1---1----11----1111-1-1---
-111--1111-11---111-1-111---1111---1-1----1--11111-

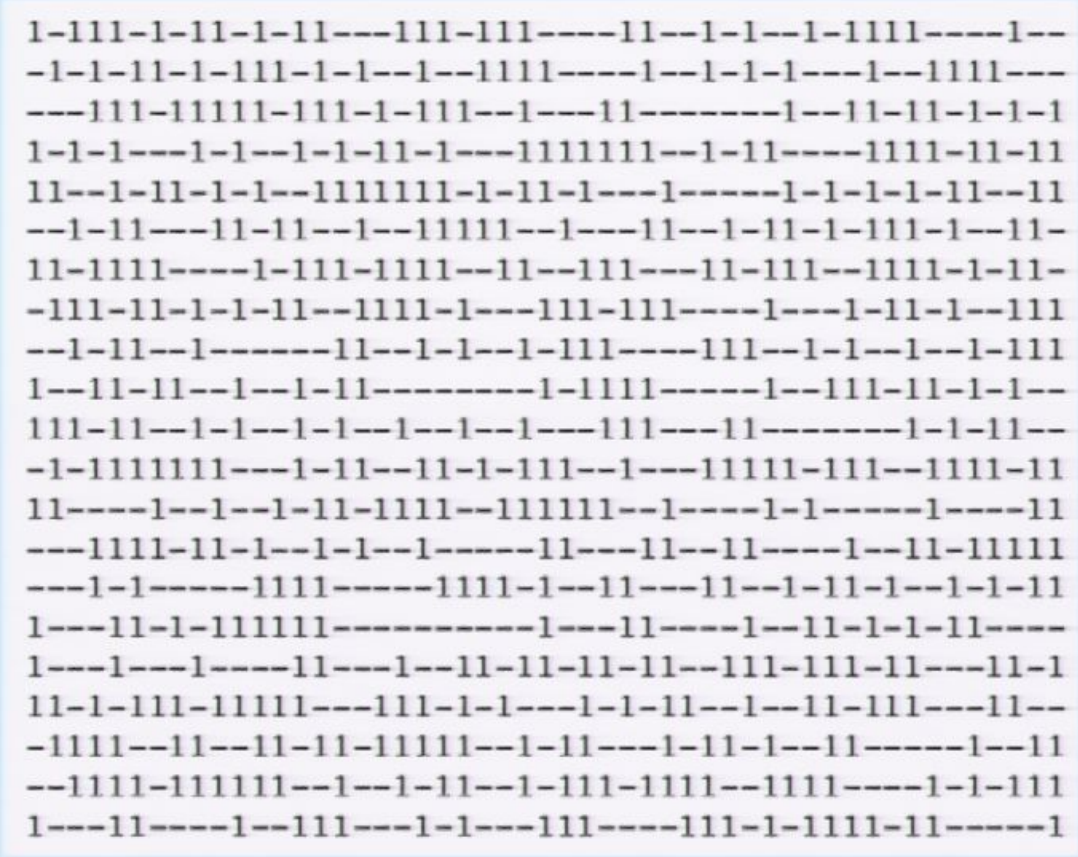
Text A


1-111-1-11-1-11---111-111----11--1-1--1-1111----1--
-1-1-11-1-111-1-1--1--1111----1--1-1-1---1--1111---
---111-11111-111-1-111--1---11-------1--11-11-1-1-1
1-1-1---1-1--1-1-11-1---1111111--1-11----1111-11-11
11--1-11-1-1--1111111-1-11-1---1-----1-1-1-1-11--11
--1-11---11-11--1--11111--1---11--1-11-1-111-1--11-
11-1111----1-111-1111--11--111---11-111--1111-1-11-
-111-11-1-1-11--1111-1---111-111----1---1-11-1--111
--1-11--1------11--1-1--1-111----111--1-1--1--1-111
1--11-11--1--1-11--------1-1111-----1--111-11-1-1--
111-11--1-1--1-1--1--1--1---111---11-------1-1-11--
-1-1111111---1-11--11-1-111--1---11111-111--1111-11
11----1--1--1-11-1111--111111--1----1-1-----1----11
---1111-11-1--1-1--1-----11---11--11----1--11-11111
---1-1-----1111-----1111-1--11---11--1-11-1--1-1-11
1---11-1-111111----------1---11----1--11-1-1-11----
1---1---1----11---1--11-11-11-11--111-111-11---11-1
11-1-111-11111---111-1-1---1-1-11--1--11-111---11--
-1111--11--11-11-11111--1-11---1-11-1--11-----1--11
--1111-111111--1--1-11--1-111-1111--1111----1-1-111
1---11----1--111---1-1---111----111-1-1111-11-----1

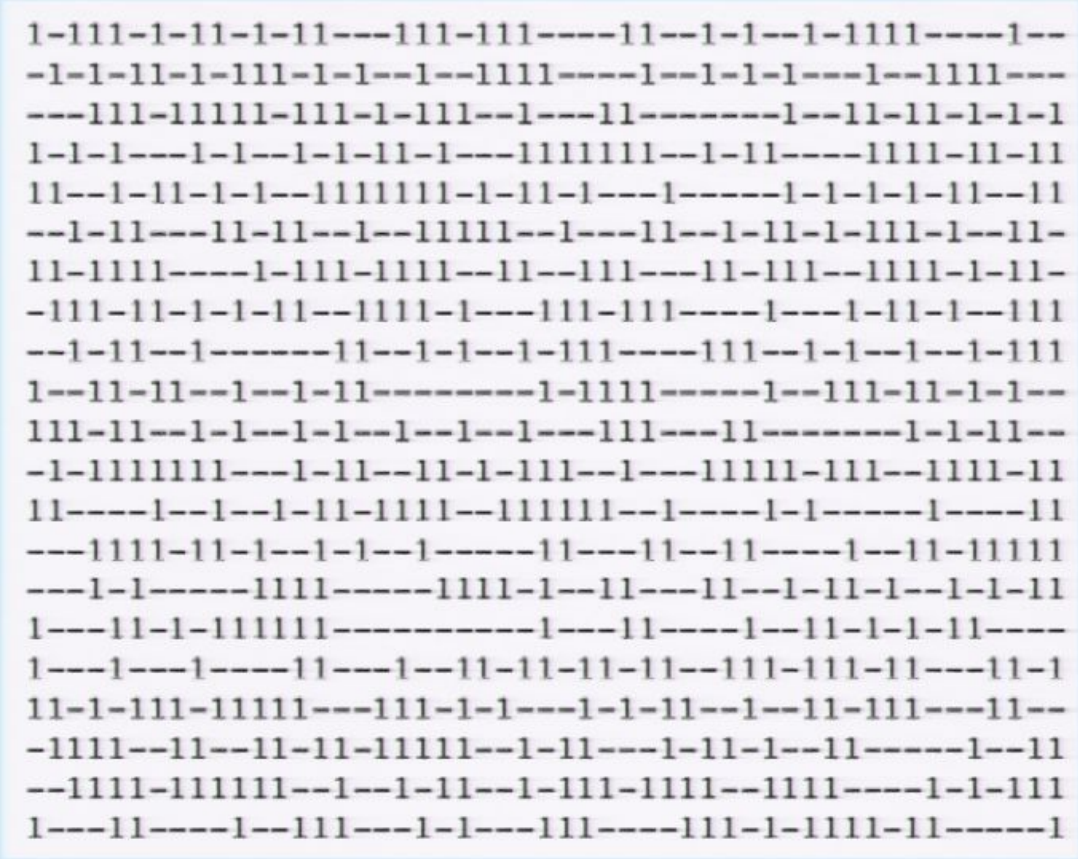
Text B


-1---1-1--1-1--111---1---1111--11-1-11-1----1111-11
1-1-1--1-1---1-1-11-11----1111-11-1-1-111-11----111
111---1-----1---1-1---11-111--1111111-11--1--1-1-1-
-1-1-111-1-11-1-1--1-111-------11-1--1111----1--1--
--11-1--1-1-11-------1-1--1-111-11111-1-1-1-1--11--
11-1--111--1--11-11-----11-111--11-1--1-1---1-11--1
--1----1111-1---1----11--11---111--1---11----1-1--1
1---1--1-1-1--11----1-111---1---1111-111-1--1-11---
11-1--11-111111--11-1-11-1---1111---11-1-11-11-1---
-11--1--11-11-1--11111111-1----11111-11---1--1-1-11
---1--11-1-11-1-11-11-11-111---111--1111111-1-1--11
1-1-----111-1--11--1-1---11-111------1---11----1--
--1111-11-11-1--1----11------11-1111-1-11111-1111--
111----1--1-11-1-11-11111--111--11--1111-11--1-----
111-1-11111----11111----1-11--111--11-1--1-11-1-1--
-111--1-1------1111111111-111--1111-11--1-1-1--1111
-111-111-1111--111-11--1--1--1--11---1---1--111--1-
--1-1---1-----111---1-1-111-1-1--11-11--1---111--11
1----11--11--1--1-----11-1--111-1--1-11--11111-11--
11----1------11-11-1--11-1---1----11----1111-1-1---
-111--1111-11---111-1-111---1111---1-1----1--11111-

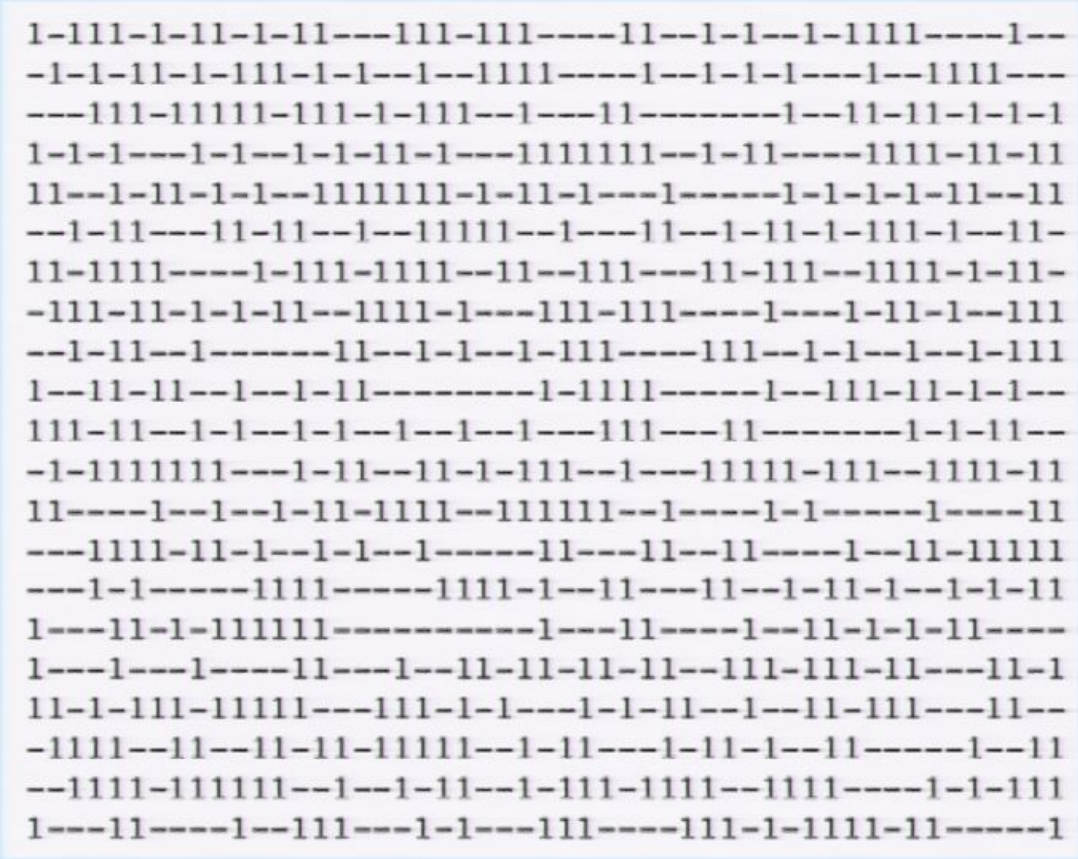
Text A


1-111-1-11-1-11---111-111----11--1-1--1-1111----1--
-1-1-11-1-111-1-1--1--1111----1--1-1-1---1--1111---
---111-11111-111-1-111--1---11-------1--11-11-1-1-1
1-1-1---1-1--1-1-11-1---1111111--1-11----1111-11-11
11--1-11-1-1--1111111-1-11-1---1-----1-1-1-1-11--11
--1-11---11-11--1--11111--1---11--1-11-1-111-1--11-
11-1111----1-111-1111--11--111---11-111--1111-1-11-
-111-11-1-1-11--1111-1---111-111----1---1-11-1--111
--1-11--1------11--1-1--1-111----111--1-1--1--1-111
1--11-11--1--1-11--------1-1111-----1--111-11-1-1--
111-11--1-1--1-1--1--1--1---111---11-------1-1-11--
-1-1111111---1-11--11-1-111--1---11111-111--1111-11
11----1--1--1-11-1111--111111--1----1-1-----1----11
---1111-11-1--1-1--1-----11---11--11----1--11-11111
---1-1-----1111-----1111-1--11---11--1-11-1--1-1-11
1---11-1-111111----------1---11----1--11-1-1-11----
1---1---1----11---1--11-11-11-11--111-111-11---11-1
11-1-111-11111---111-1-1---1-1-11--1--11-111---11--
-1111--11--11-11-11111--1-11---1-11-1--11-----1--11
--1111-111111--1--1-11--1-111-1111--1111----1-1-111
1---11----1--111---1-1---111----111-1-1111-11-----1

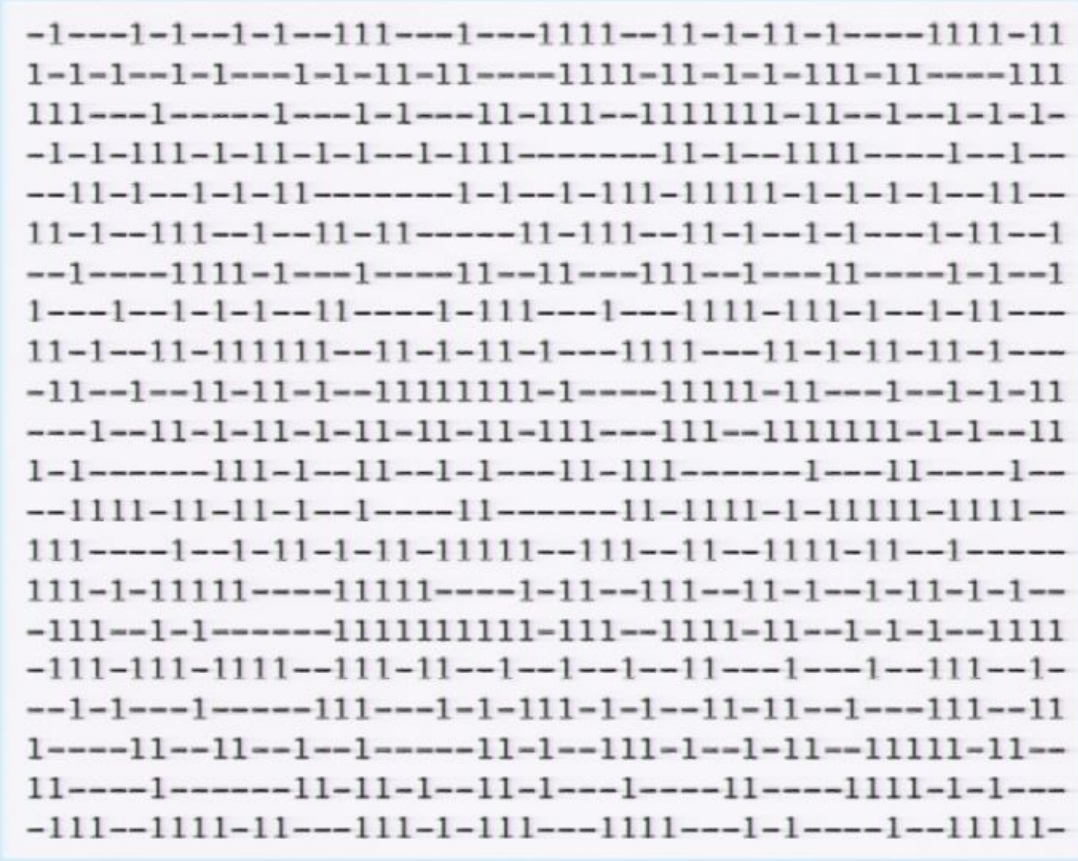
Text A



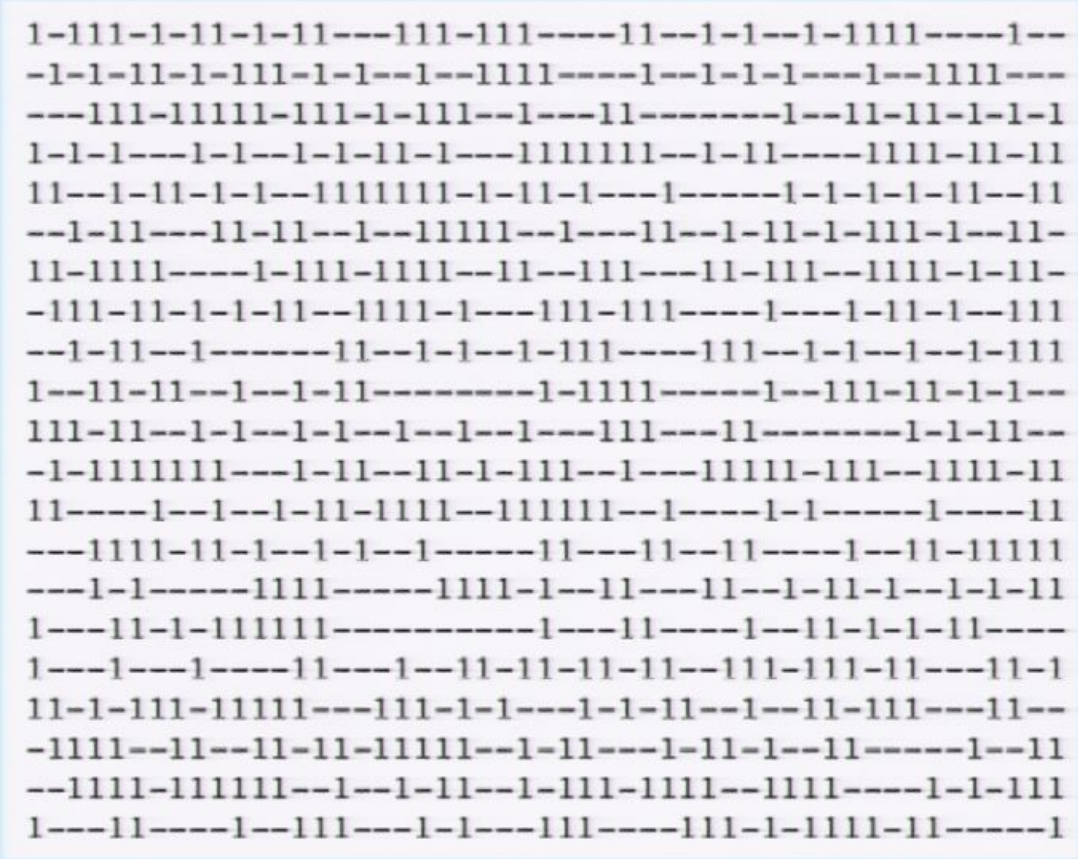
Text A



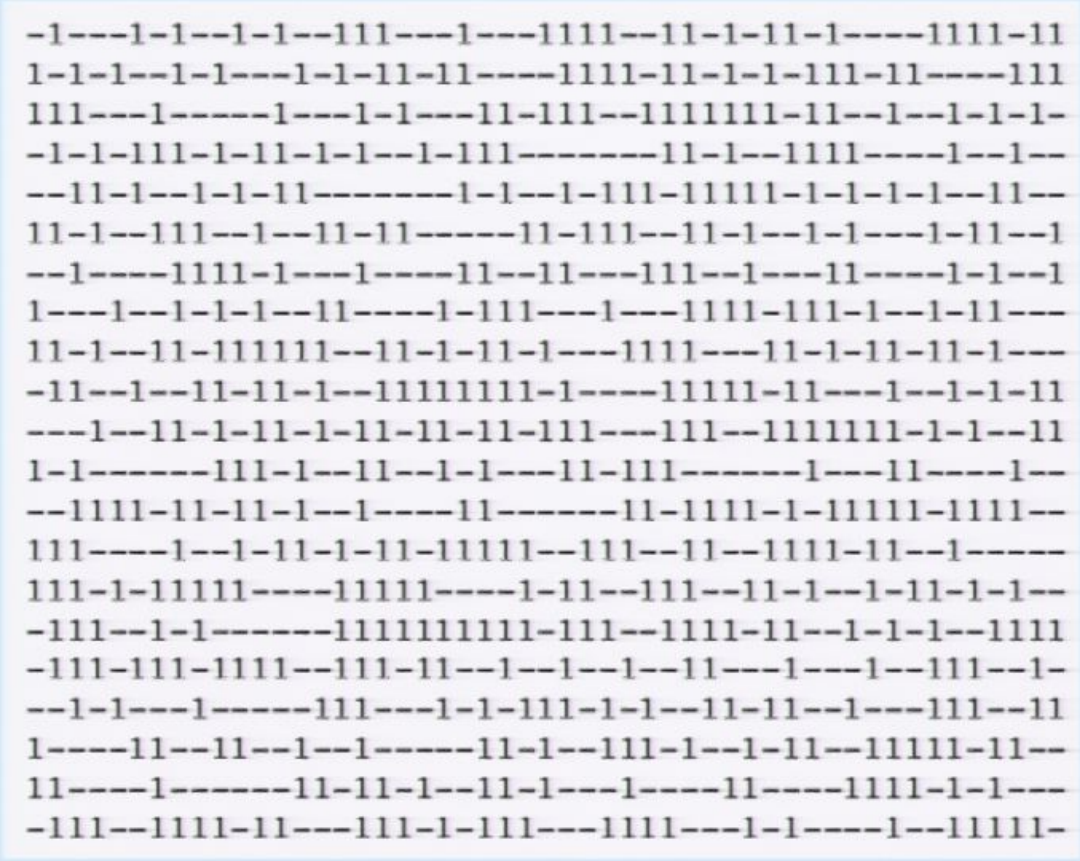
Text B


-1---1-1--1-1--111---1---1111--11-1-11-1----1111-11
1-1-1--1-1---1-1-11-11----1111-11-1-1-111-11----111
111---1-----1---1-1---11-111--1111111-11--1--1-1-1-
-1-1-111-1-11-1-1--1-111-------11-1--1111----1--1--
--11-1--1-1-11-------1-1--1-111-11111-1-1-1-1--11--
11-1--111--1--11-11-----11-111--11-1--1-1---1-11--1
--1----1111-1---1----11--11---111--1---11----1-1--1
1---1--1-1-1--11----1-111---1---1111-111-1--1-11---
11-1--11-111111--11-1-11-1---1111---11-1-11-11-1---
-11--1--11-11-1--11111111-1----11111-11---1--1-1-11
---1--11-1-11-1-11-11-11-111---111--1111111-1-1--11
1-1-----111-1--11--1-1---11-111------1---11----1--
--1111-11-11-1--1----11------11-1111-1-11111-1111--
111----1--1-11-1-11-11111--111--11--1111-11--1-----
111-1-11111----11111----1-11--111--11-1--1-11-1-1--
-111--1-1------1111111111-111--1111-11--1-1-1--1111
-111-111-1111--111-11--1--1--1--11---1---1--111--1-
--1-1---1-----111---1-1-111-1-1--11-11--1---111--11
1----11--11--1--1-----11-1--111-1--1-11--11111-11--
11----1------11-11-1--11-1---1----11----1111-1-1---
-111--1111-11---111-1-111---1111---1-1----1--11111-

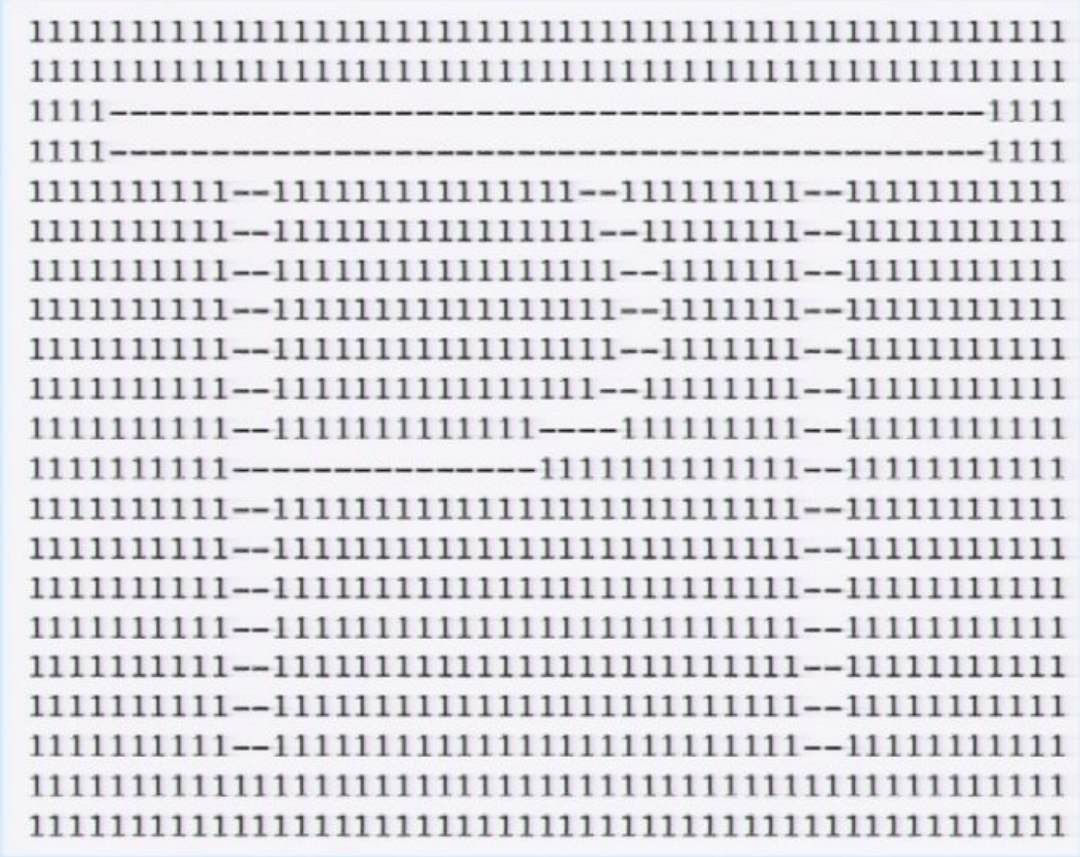
Text A


1-111-1-11-1-11---111-111----11--1-1--1-1111----1--
-1-1-11-1-111-1-1--1--1111----1--1-1-1---1--1111---
---111-11111-111-1-111--1---11-------1--11-11-1-1-1
1-1-1---1-1--1-1-11-1---1111111--1-11----1111-11-11
11--1-11-1-1--1111111-1-11-1---1-----1-1-1-1-11--11
--1-11---11-11--1--11111--1---11--1-11-1-111-1--11-
11-1111----1-111-1111--11--111---11-111--1111-1-11-
-111-11-1-1-11--1111-1---111-111----1---1-11-1--111
--1-11--1------11--1-1--1-111----111--1-1--1--1-111
1--11-11--1--1-11--------1-1111-----1--111-11-1-1--
111-11--1-1--1-1--1--1--1---111---11-------1-1-11--
-1-1111111---1-11--11-1-111--1---11111-111--1111-11
11----1--1--1-11-1111--111111--1----1-1-----1----11
---1111-11-1--1-1--1-----11---11--11----1--11-11111
---1-1-----1111-----1111-1--11---11--1-11-1--1-1-11
1---11-1-111111----------1---11----1--11-1-1-11----
1---1---1----11---1--11-11-11-11--111-111-11---11-1
11-1-111-11111---111-1-1---1-1-11--1--11-111---11--
-1111--11--11-11-11111--1-11---1-11-1--11-----1--11
--1111-111111--1--1-11--1-111-1111--1111----1-1-111
1---11----1--111---1-1---111----111-1-1111-11-----1

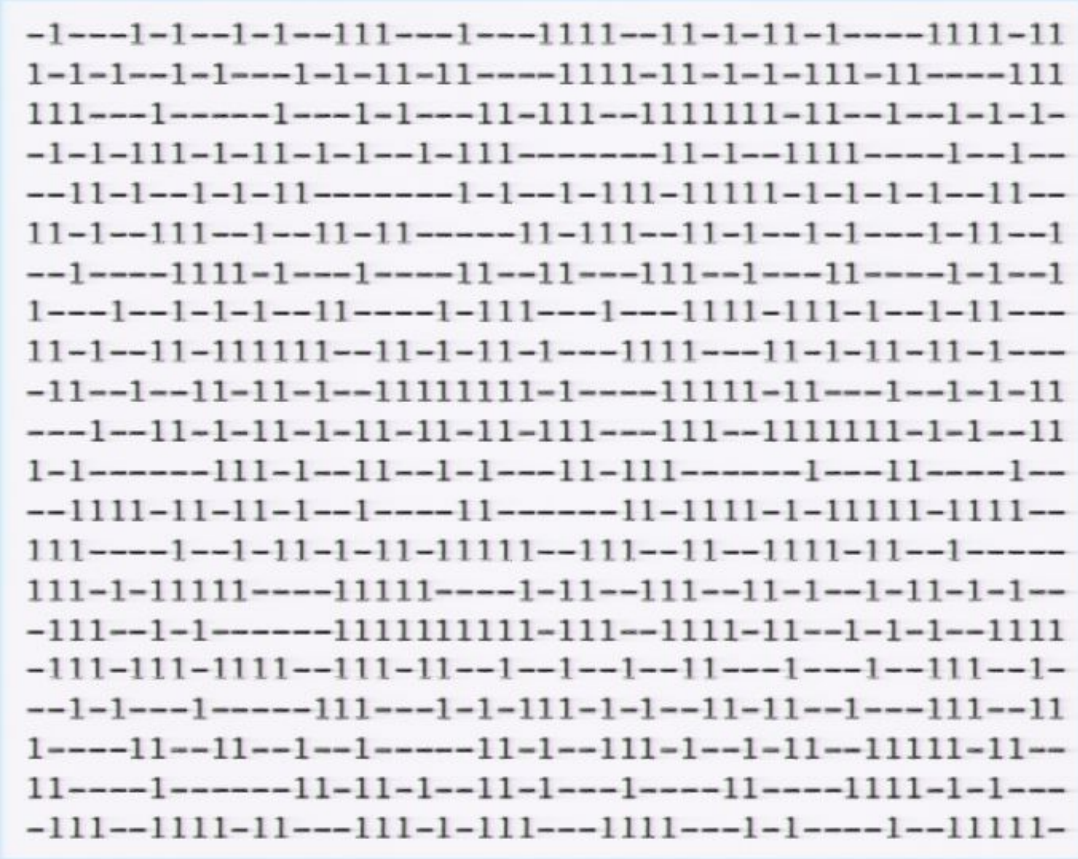
Text B


-1---1-1--1-1--111---1---1111--11-1-11-1----1111-11
1-1-1--1-1---1-1-11-11----1111-11-1-1-111-11----111
111---1-----1---1-1---11-111--1111111-11--1--1-1-1-
-1-1-111-1-11-1-1--1-111-------11-1--1111----1--1--
--11-1--1-1-11-------1-1--1-111-11111-1-1-1-1--11--
11-1--111--1--11-11-----11-111--11-1--1-1---1-11--1
--1----1111-1---1----11--11---111--1---11----1-1--1
1---1--1-1-1--11----1-111---1---1111-111-1--1-11---
11-1--11-111111--11-1-11-1---1111---11-1-11-11-1---
-11--1--11-11-1--11111111-1----11111-11---1--1-1-11
---1--11-1-11-1-11-11-11-111---111--1111111-1-1--11
1-1-----111-1--11--1-1---11-111------1---11----1--
--1111-11-11-1--1----11------11-1111-1-11111-1111--
111----1--1-11-1-11-11111--111--11--1111-11--1-----
111-1-11111----11111----1-11--111--11-1--1-11-1-1--
-111--1-1------1111111111-111--1111-11--1-1-1--1111
-111-111-1111--111-11--1--1--1--11---1---1--111--1-
--1-1---1-----111---1-1-111-1-1--11-11--1---111--11
1----11--11--1--1-----11-1--111-1--1-11--11111-11--
11----1------11-11-1--11-1---1----11----1111-1-1---
-111--1111-11---111-1-111---1111---1-1----1--11111-

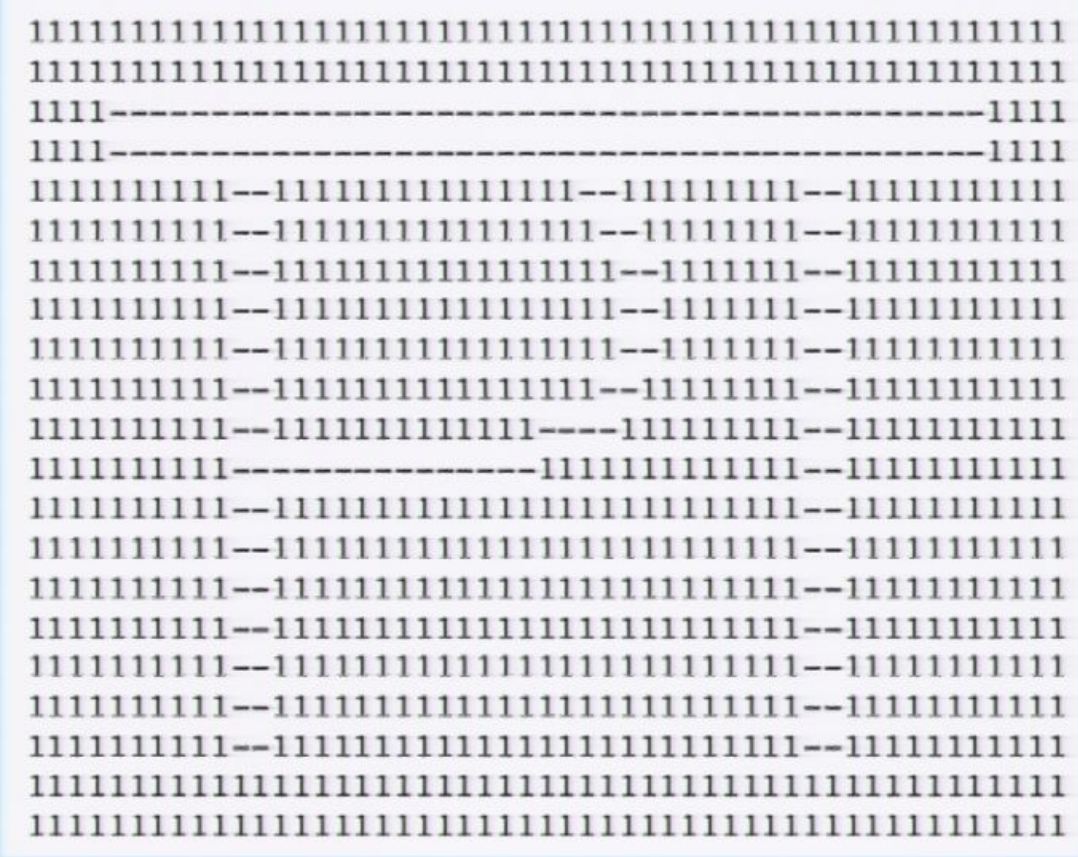
“Difference”



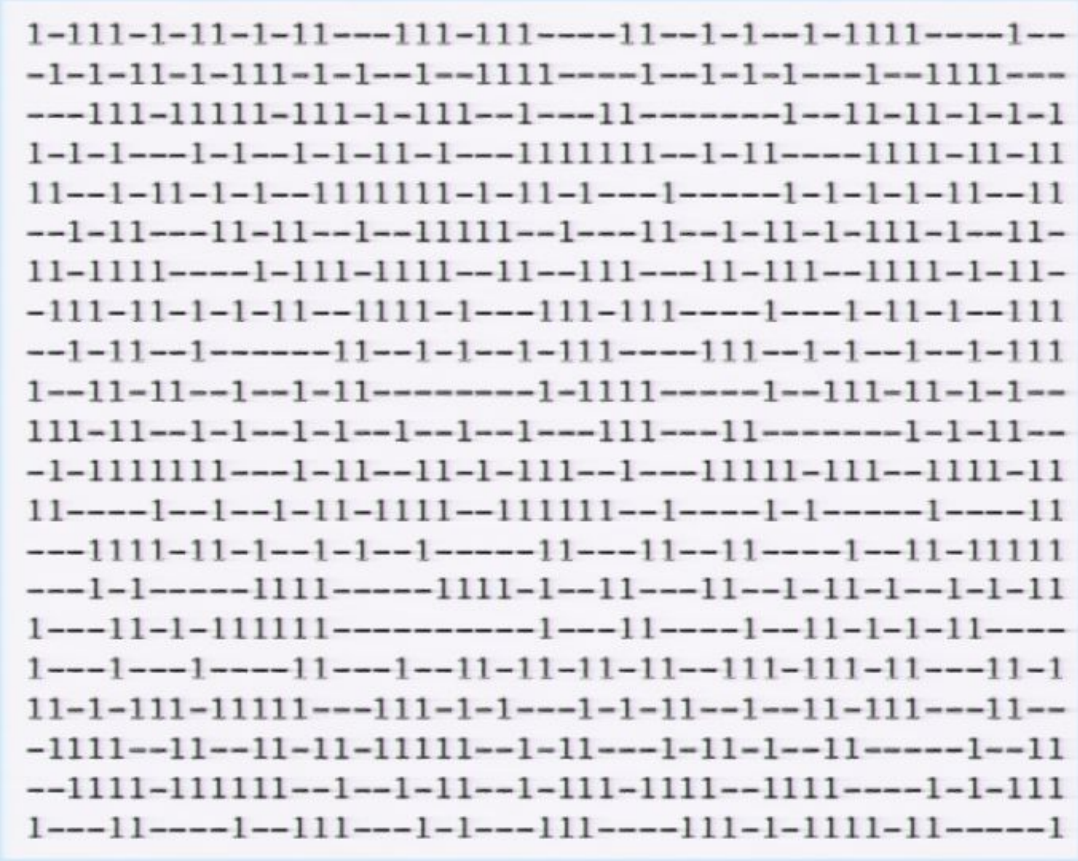
Text B


-1---1-1--1-1--111---1---1111--11-1-11-1----1111-11
1-1-1--1-1---1-1-11-11----1111-11-1-1-111-11----111
111---1-----1---1-1---11-111--1111111-11--1--1-1-1-
-1-1-111-1-11-1-1--1-111-------11-1--1111----1--1--
--11-1--1-1-11-------1-1--1-111-11111-1-1-1-1--11--
11-1--111--1--11-11-----11-111--11-1--1-1---1-11--1
--1----1111-1---1----11--11---111--1---11----1-1--1
1---1--1-1-1--11----1-111---1---1111-111-1--1-11---
11-1--11-111111--11-1-11-1---1111---11-1-11-11-1---
-11--1--11-11-1--11111111-1----11111-11---1--1-1-11
---1--11-1-11-1-11-11-11-111---111--1111111-1-1--11
1-1-----111-1--11--1-1---11-111------1---11----1--
--1111-11-11-1--1----11------11-1111-1-11111-1111--
111----1--1-11-1-11-11111--111--11--1111-11--1-----
111-1-11111----11111----1-11--111--11-1--1-11-1-1--
-111--1-1------1111111111-111--1111-11--1-1-1--1111
-111-111-1111--111-11--1--1--1--11---1---1--111--1-
--1-1---1-----111---1-1-111-1-1--11-11--1---111--11
1----11--11--1--1-----11-1--111-1--1-11--11111-11--
11----1------11-11-1--11-1---1----11----1111-1-1---
-111--1111-11---111-1-111---1111---1-1----1--11111-

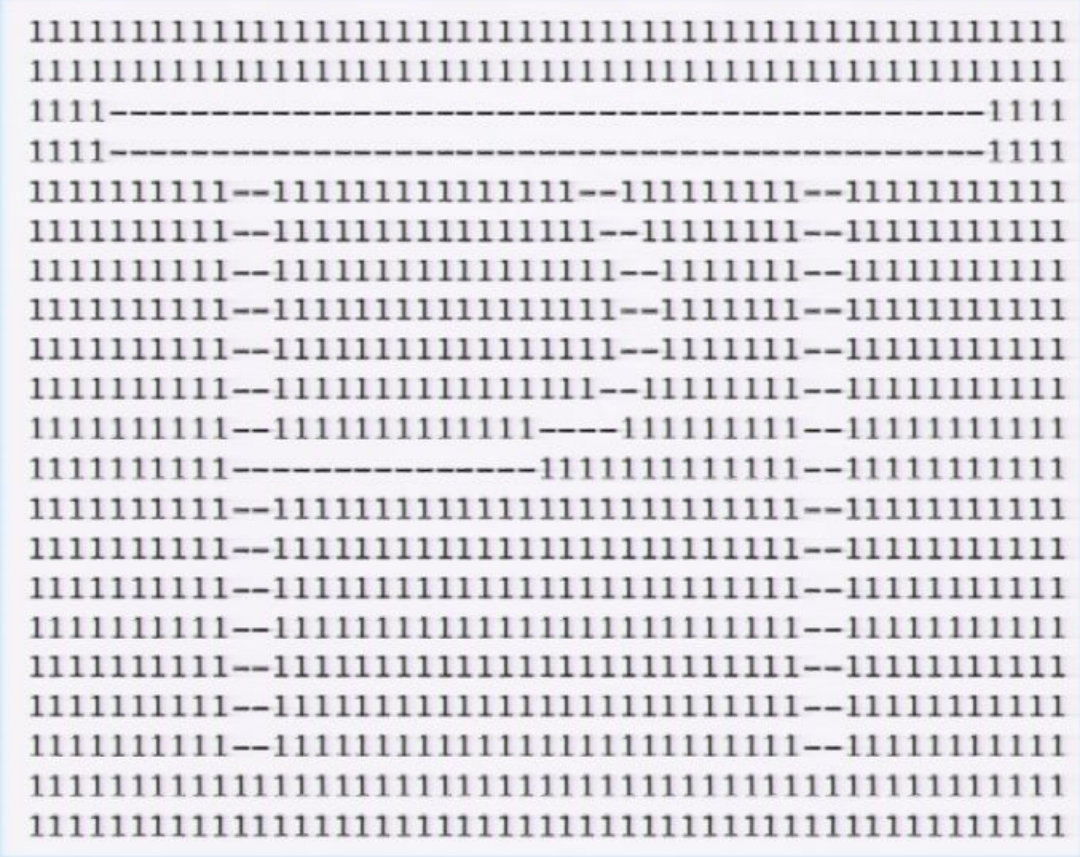
“Difference”


1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111--1111
1111--1111
111111111--111111111111111--11111111--1111111111
111111111--111111111111111--11111111--1111111111
111111111--111111111111111--1111111--1111111111
111111111--111111111111111--1111111--1111111111
111111111--111111111111111--1111111--1111111111
111111111--111111111111111--11111111--1111111111
111111111--1111111111111----11111111--1111111111
111111111--------------1111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111

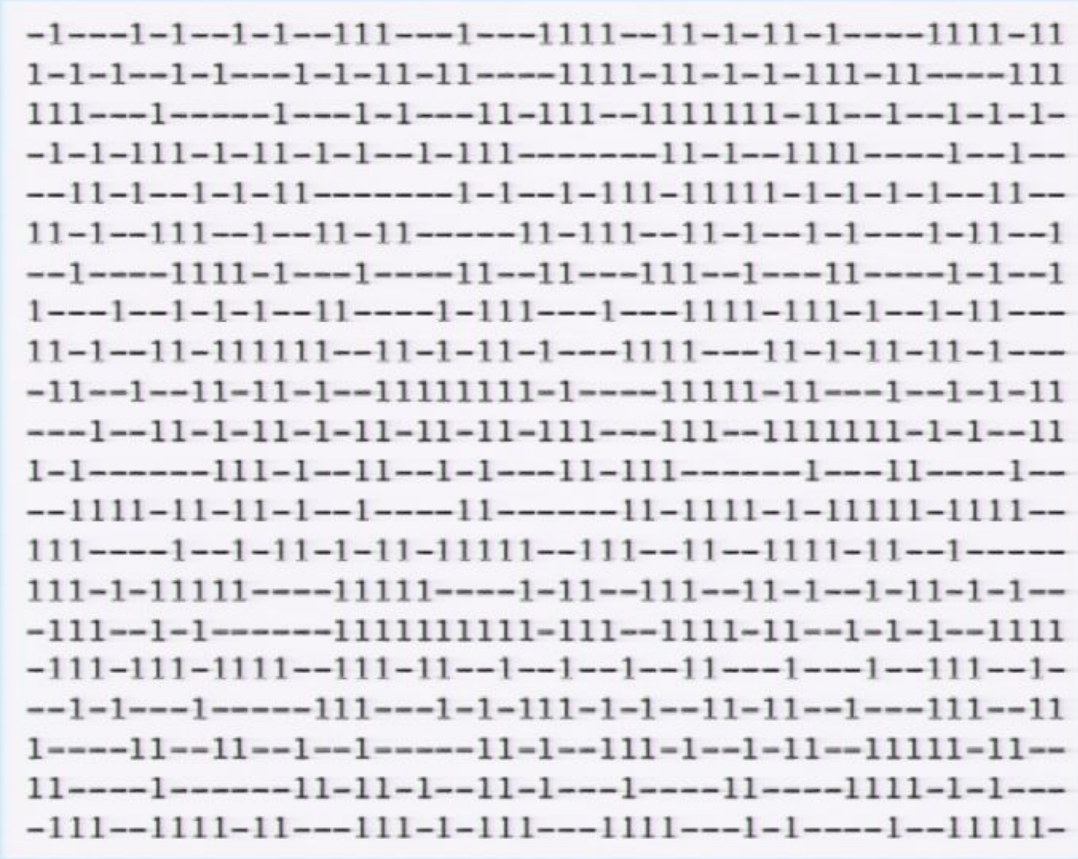
Text A


1-111-1-11-1-11---111-111----11--1-1--1-1111----1--
-1-1-11-1-111-1-1--1--1111----1--1-1-1---1--1111---
---111-11111-111-1-111--1---11-------1--11-11-1-1-1
1-1-1---1-1--1-1-11-1---1111111--1-11----1111-11-11
11--1-11-1-1--1111111-1-11-1---1-----1-1-1-1-11--11
--1-11---11-11--1--11111--1---11--1-11-1-111-1--11-
11-1111----1-111-1111--11--111---11-111--1111-1-11-
-111-11-1-1-11--1111-1---111-111----1---1-11-1--111
--1-11--1------11--1-1--1-111----111--1-1--1--1-111
1--11-11--1--1-11--------1-1111-----1--111-11-1-1--
111-11--1-1--1-1--1--1--1---111---11-------1-1-11--
-1-1111111---1-11--11-1-111--1---11111-111--1111-11
11----1--1--1-11-1111--111111--1----1-1-----1----11
---1111-11-1--1-1--1-----11---11--11----1--11-11111
---1-1-----1111-----1111-1--11---11--1-11-1--1-1-11
1---11-1-111111----------1---11----1--11-1-1-11----
1---1---1----11---1--11-11-11-11--111-111-11---11-1
11-1-111-11111---111-1-1---1-1-11--1--11-111---11--
-1111--11--11-11-11111--1-11---1-11-1--11-----1--11
--1111-111111--1--1-11--1-111-1111--1111----1-1-111
1---11----1--111---1-1---111----111-1-1111-11-----1

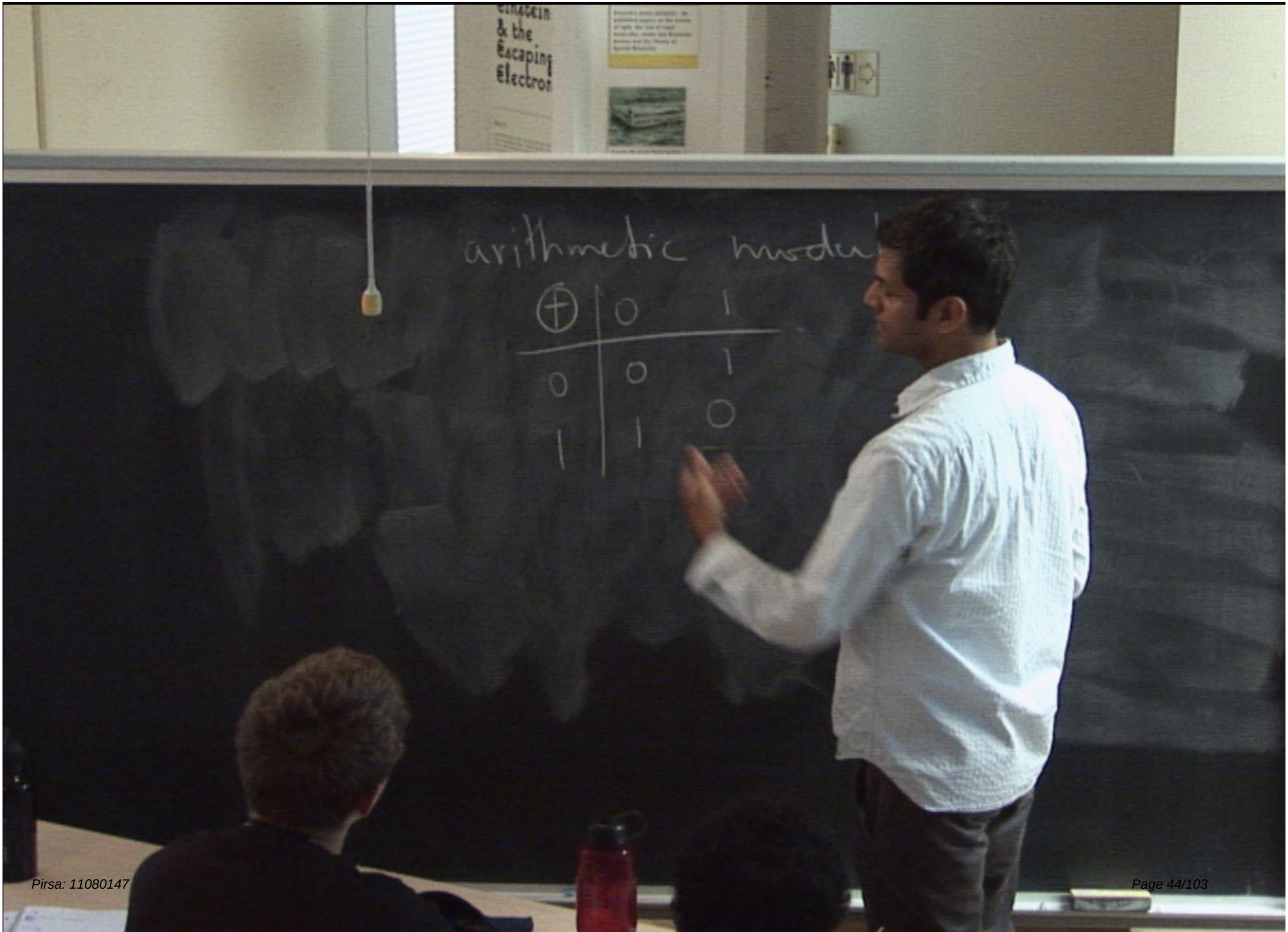
“Difference”

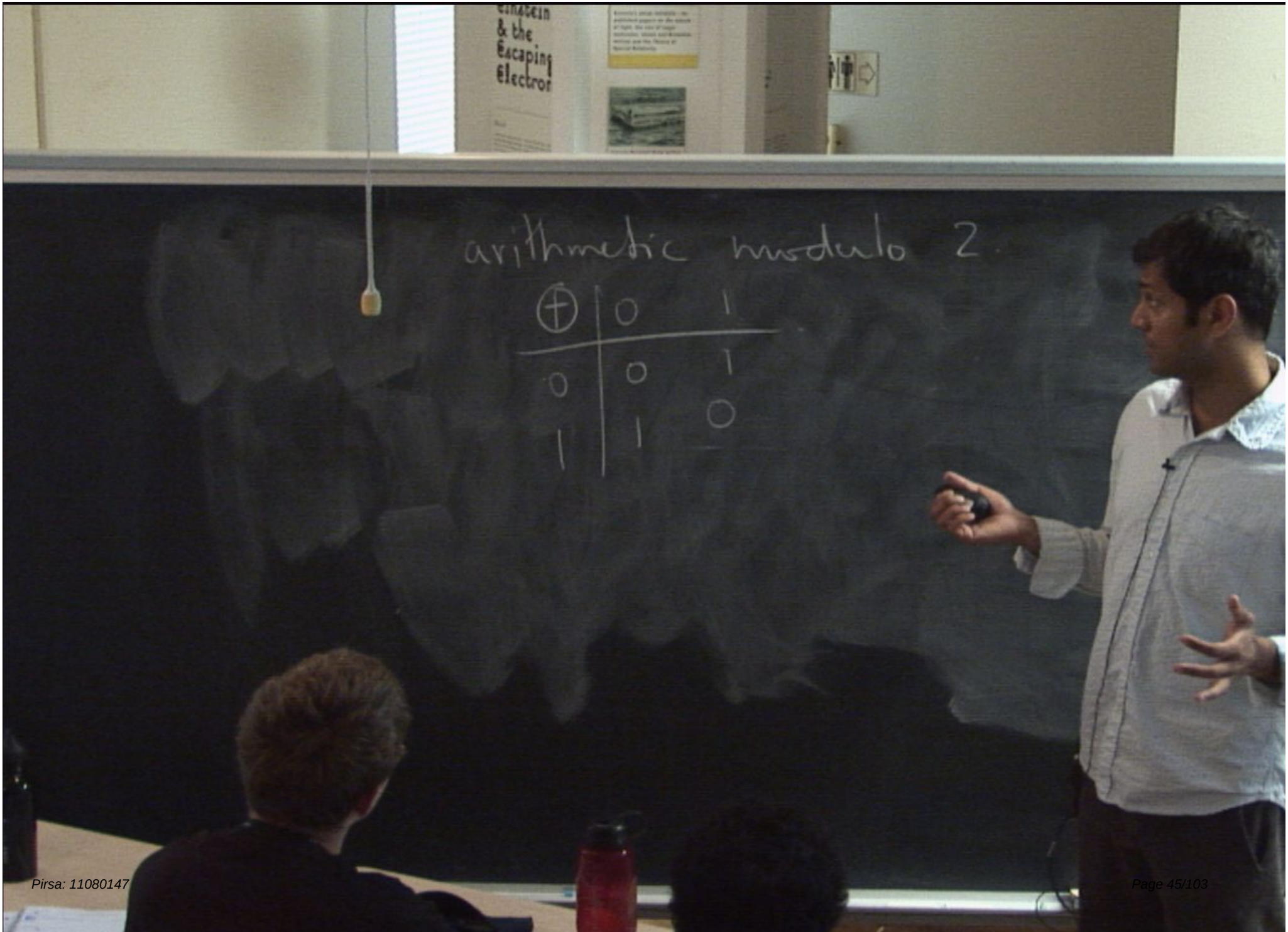

1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111--1111
1111--1111
111111111--111111111111111--11111111--1111111111
111111111--111111111111111--11111111--1111111111
111111111--111111111111111--1111111--1111111111
111111111--111111111111111--1111111--1111111111
111111111--111111111111111--1111111--1111111111
111111111--111111111111111--11111111--1111111111
111111111--111111111111----11111111--1111111111
111111111--------------111111111111--1111111111
111111111--11111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--11111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--11111111111111111111111--1111111111
111111111--111111111111111111111111--1111111111
111111111--11111111111111111111111--1111111111
111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111

Text B


-1---1-1--1-1--111---1---1111--11-1-11-1----1111-11
1-1-1--1-1---1-1-11-11----1111-11-1-1-111-11----111
111---1-----1---1-1---11-111--1111111-11--1--1-1-1-
-1-1-111-1-11-1-1--1-111-------11-1--1111----1--1--
--11-1--1-1-11-------1-1--1-111-11111-1-1-1-1--11--
11-1--111--1--11-11-----11-111--11-1--1-1---1-11--1
--1----1111-1---1----11--11---111--1---11----1-1--1
1---1--1-1-1--11----1-111---1---1111-111-1--1-11---
11-1--11-111111--11-1-11-1---1111---11-1-11-11-1---
-11--1--11-11-1--11111111-1----11111-11---1--1-1-11
---1--11-1-11-1-11-11-11-111---111--1111111-1-1--11
1-1-----111-1--11--1-1---11-111------1---11----1--
--1111-11-11-1--1----11------11-1111-1-11111-1111--
111----1--1-11-1-11-11111--111--11--1111-11--1-----
111-1-11111----11111----1-11--111--11-1--1-11-1-1--
-111--1-1------1111111111-111--1111-11--1-1-1--1111
-111-111-1111--111-11--1--1--1--11---1---1--111--1-
--1-1---1-----111---1-1-111-1-1--11-11--1---111--11
1----11--11--1--1-----11-1--111-1--1-11--11111-11--
11----1------11-11-1--11-1---1----11----1111-1-1---
-111--1111-11---111-1-111---1111---1-1----1--11111-


PERIMETER
INSTITUTE FOR THEORETICAL PHYSICS


& the
Escaping
Electron
arithmetic
⊕ 0 1
0 0 1
1 1 0


& the
Escaping
Electron
arithmetic modulo 2
⊕ 0 1
0 0 1
1 1 0

Vernam cipher

- Idea: make ciphertext look random to others
- Alice and Bob keep outcome k of coin toss (0/1)
- Let Alice's message be a single bit m (0/1)
- Ciphertext $c = m \oplus k$

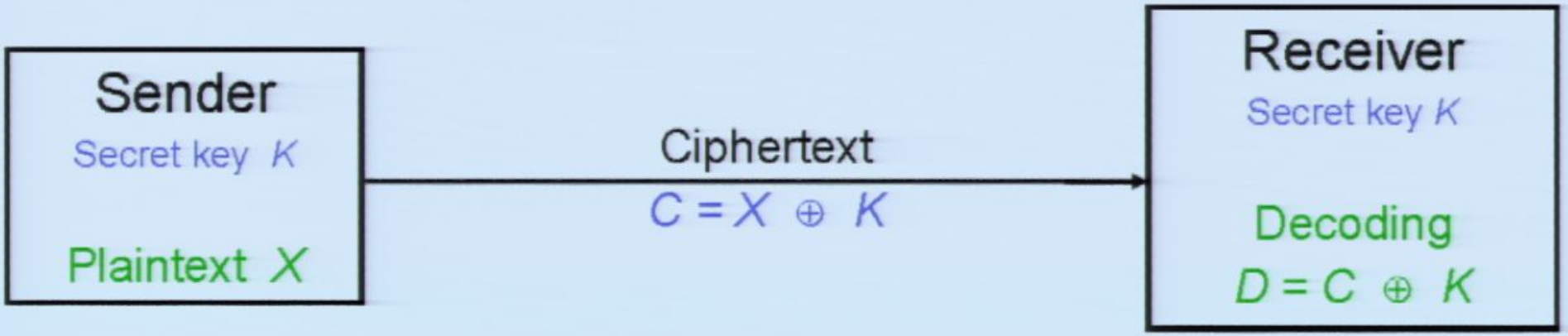
$m \setminus k$	0	1
0	0	1
1	1	0

Security

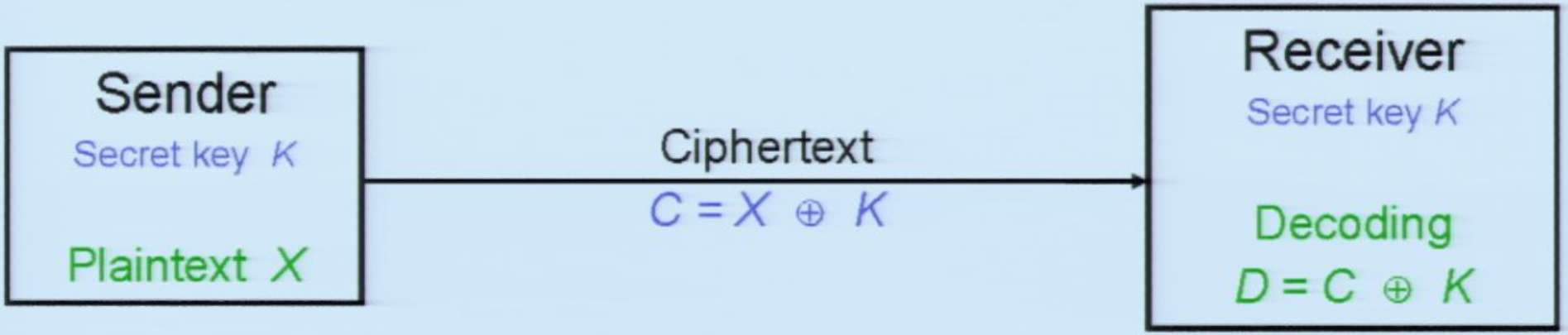
$m \setminus k$	0	1
0	0	1
1	1	0

- If k is 0 or 1 with probability 1/2, so is c !
- Ciphertext is random to all but Alice and Bob
- Bob can recover $m = c \oplus k$
- Generalizes to longer messages (apply to every bit)

Private key encryption

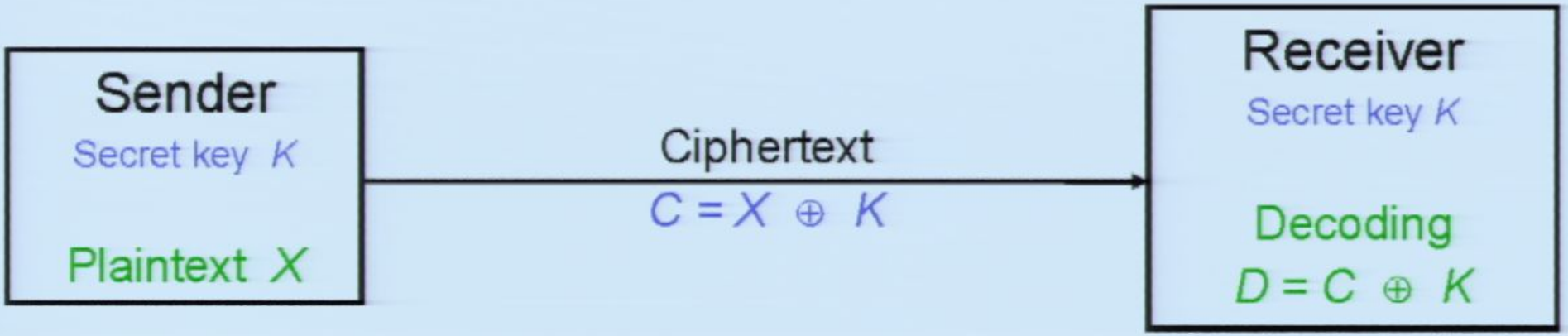


Private key encryption



Secure, unless eavesdropper knows the random key

Private key encryption

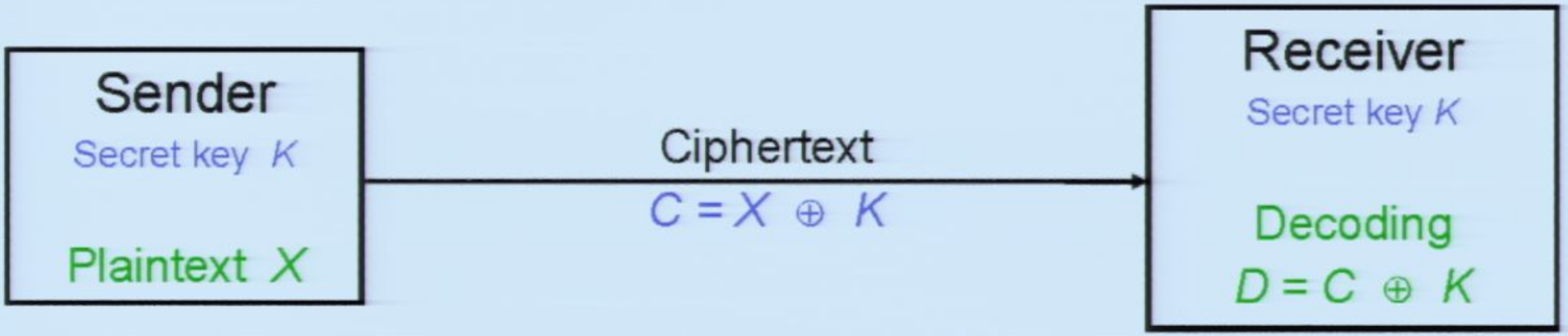


Secure, unless eavesdropper knows the random key

[Shannon 1949]

Disadvantages:

Private key encryption



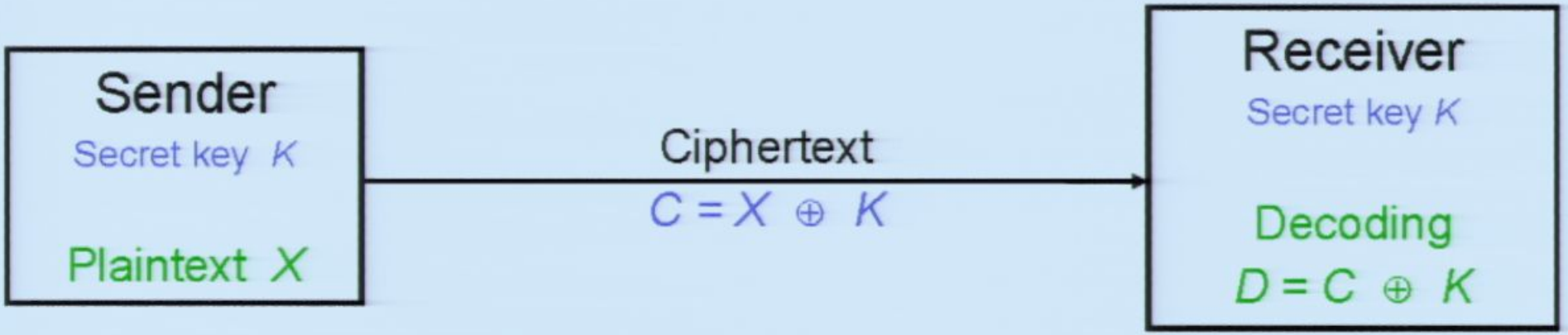
Secure, unless eavesdropper knows the random key

[Shannon 1949]

Disadvantages:

(1) n users $\rightarrow n(n-1)/2$ keys

Private key encryption



Secure, unless eavesdropper knows the random key

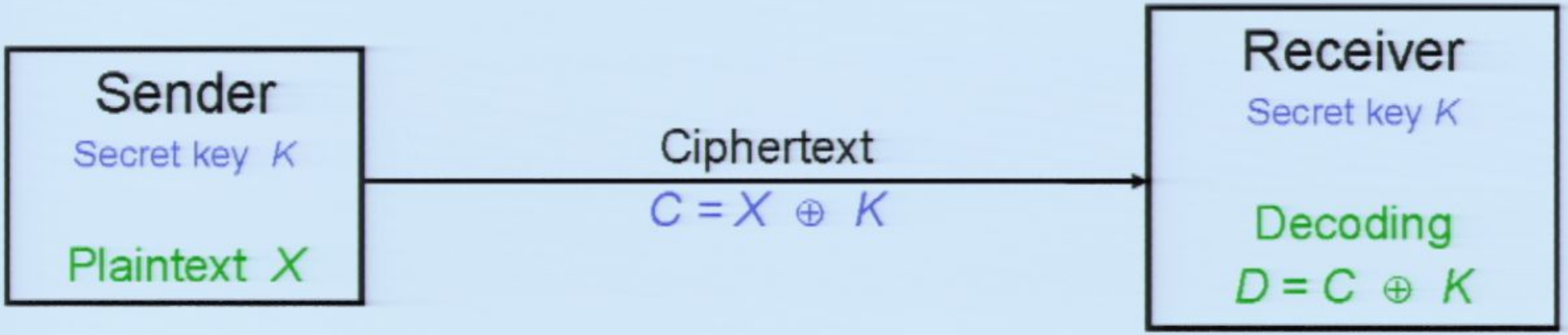
[Shannon 1949]

Disadvantages:

(1) n users $\rightarrow n(n\text{-}1)/2$ keys

(2) Cannot reuse

Private key encryption



Secure, unless eavesdropper knows the random key

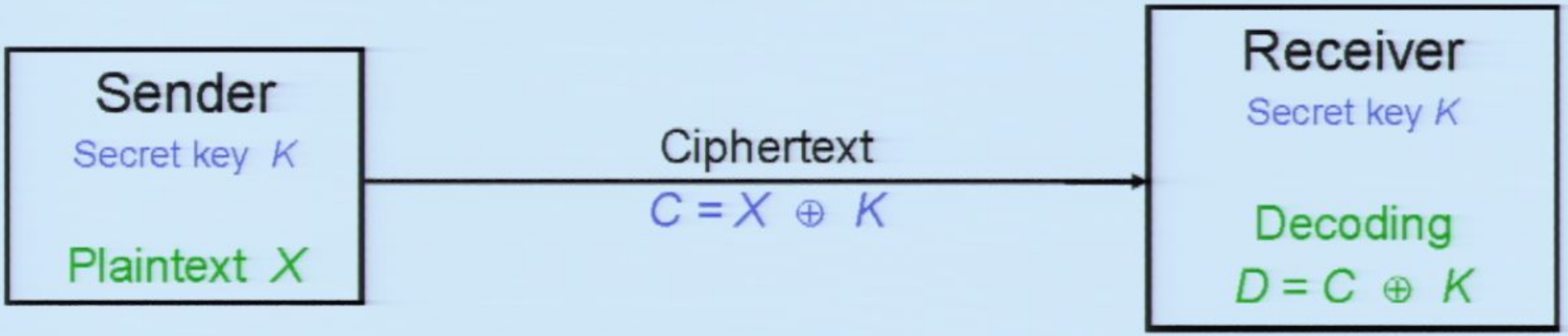
[Shannon 1949]

Disadvantages:

(1) n users $\rightarrow n(n\text{-}1)/2$ keys
(2) Cannot reuse
(3) Users have to meet physically to share keys

Use of photon polarization

Private key encryption



Secure, unless eavesdropper knows the random key

[Shannon 1949]

Disadvantages:

(1) n users $\rightarrow n(n-1)/2$ keys
(2) Cannot reuse
(3) Users have to meet physically to share keys

Use of photon polarization

- Enables remote key agreement…

  …and therefore private key encryption

Use of photon polarization

- Enables remote key agreement…
  …and therefore private key encryption

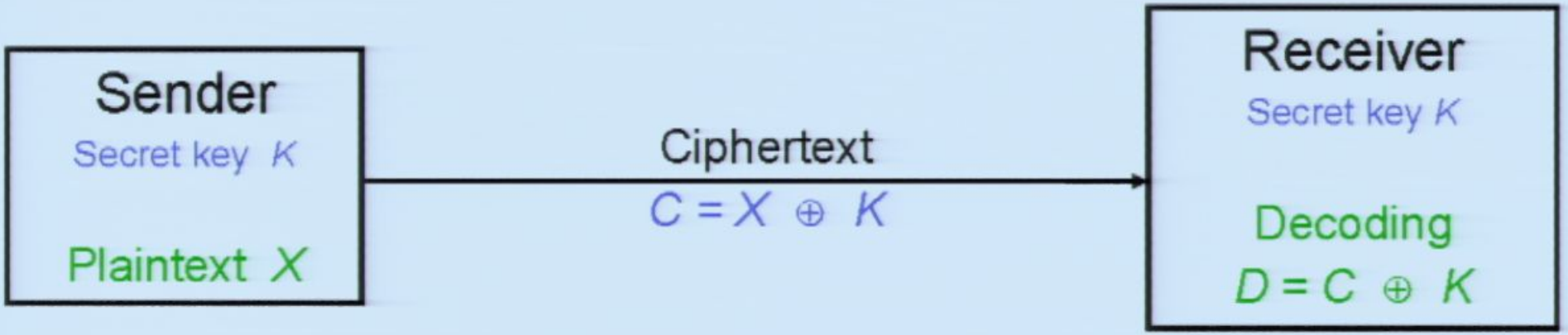
- Internet transactions are based on public key encryption

Use of photon polarization

- Enables remote key agreement…

  …and therefore private key encryption

Private key encryption



Secure, unless eavesdropper knows the random key

[Shannon 1949]

Disadvantages:

(1) n users $\rightarrow n(n-1)/2$ keys
(2) Cannot reuse
(3) Users have to meet physically to share keys

Use of photon polarization

- Enables remote key agreement…

  …and therefore private key encryption

Use of photon polarization

- Enables remote key agreement…
  …and therefore private key encryption

- Internet transactions are based on public key encryption
- Assumes computational hardness of factorizing large integers into their prime factors

- Using polarized light, we can establish a secure random key: an eavesdropper provably has little information about the key

Quantum key distribution [Bennett, Brassard'84]

Quantum key distribution [Bennett, Brassard'84]

- Assume Alice and Bob want 1 bit of key

Quantum key distribution [Bennett, Brassard'84]

- Assume Alice and Bob want 1 bit of key
- Alice picks a random bit, 0 or 1

Quantum key distribution [Bennett, Brassard'84]

- Assume Alice and Bob want 1 bit of key

- Alice picks a random bit, 0 or 1
- She also picks a random orientation, rectilinear or diagonal

Quantum key distribution [Bennett, Brassard'84]

- Assume Alice and Bob want 1 bit of key

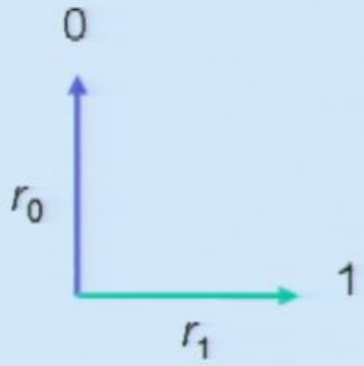
- Alice picks a random bit, 0 or 1
- She also picks a random orientation, rectilinear or diagonal

- She prepares a single photon of light with the corresponding polarization, sends it to Bob

Encoding a bit into polarization

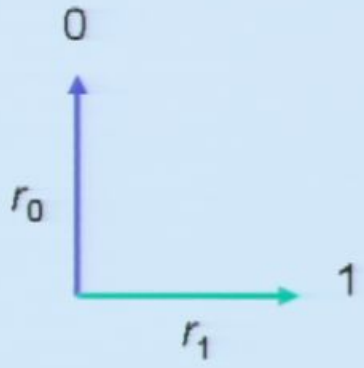
Encoding a bit into polarization

Rectilinear

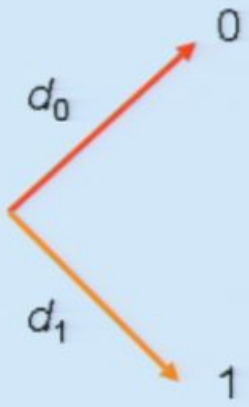


Encoding a bit into polarization

Rectilinear



Diagonal



The remaining procedure

The remaining procedure

- Bob doesn't know the bit or the orientation
- Bob picks a random orientation to measure polarization

The remaining procedure

- Bob doesn't know the bit or the orientation
- Bob picks a random orientation to measure polarization

  (has 50-50 chance of getting it and the key right)

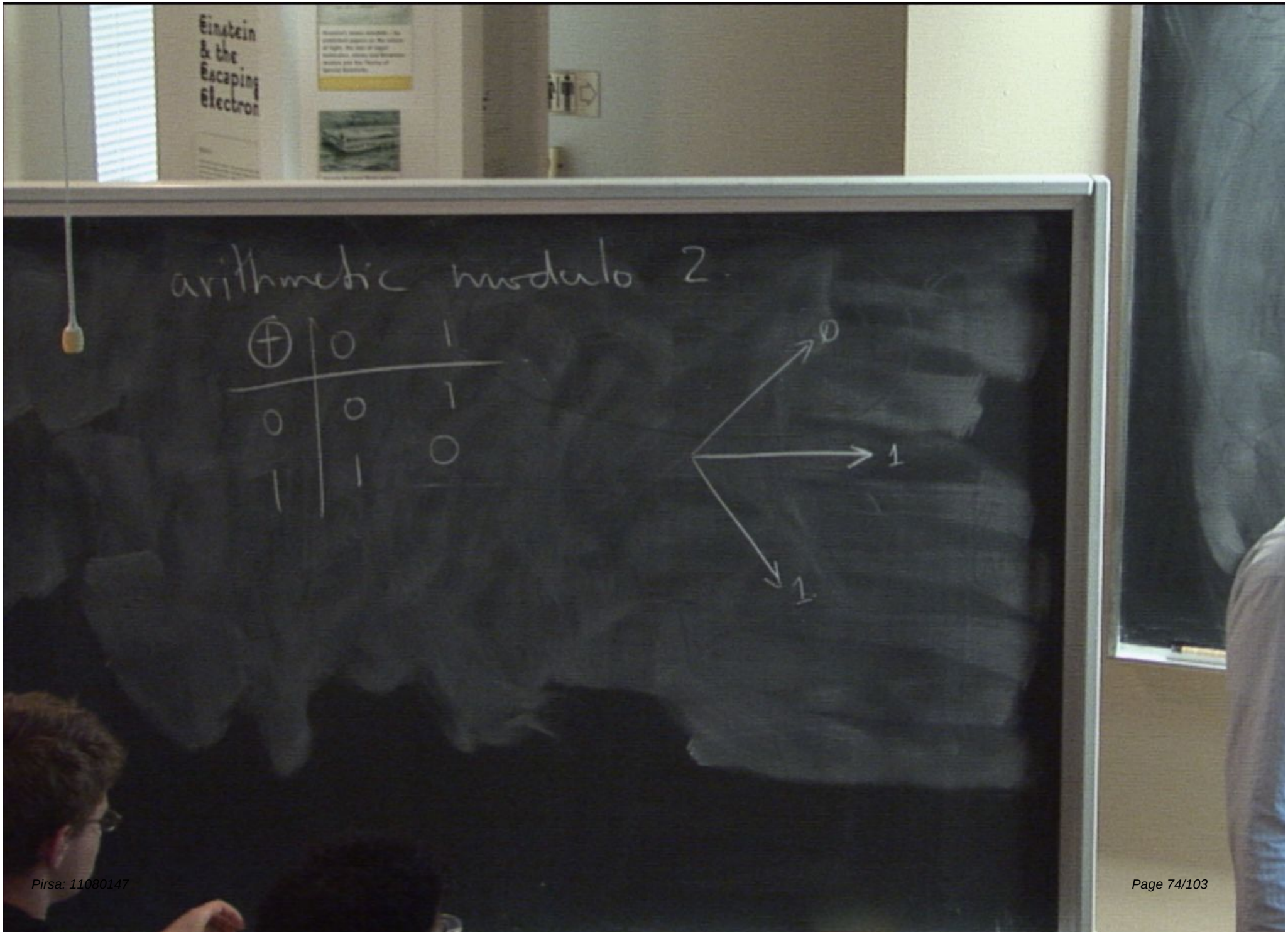
The remaining procedure

- Bob doesn't know the bit or the orientation
- Bob picks a random orientation to measure polarization

  (has 50-50 chance of getting it and the key right)

- Bob announces that he has measured

  Alice announces the orientation (but not the key bit!)


Einstein
& the
Escaping
Electron
arithmetic modulo 2
⊕ | 0 1
0 | 0 1
1 | 1 0
0
1
1

The remaining procedure

- Bob doesn't know the bit or the orientation
- Bob picks a random orientation to measure polarization

  (has 50-50 chance of getting it and the key right)

- Bob announces that he has measured

  Alice announces the orientation (but not the key bit!)

The remaining procedure

- Bob doesn't know the bit or the orientation
- Bob picks a random orientation to measure polarization

  (has 50-50 chance of getting it and the key right)

- Bob announces that he has measured

  Alice announces the orientation (but not the key bit!)

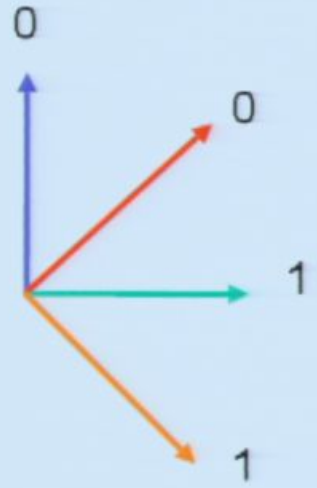
  Bob knows if he got the key bit

- If there is no eavesdropping, they have a random bit

Security against eavesdropping

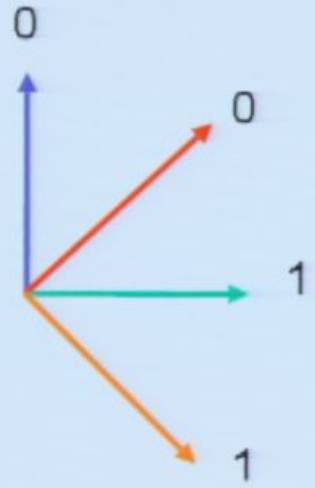
Security against eavesdropping

- If Eve tries to measure polarization, she likely alters it



Security against eavesdropping

- If Eve tries to measure polarization, she likely alters it



- Alice and Bob try to detect errors
  - Repeat encoding procedure for many key bits
  - Pick random subset for testing: Alice announces the key bit as well, and Bob checks for tampering
  - If too many bits are corrupted, they restart the protocol

Security…

Security…

- Security based only on the validity of laws of nature;

Security…

- Security based only on the validity of laws of nature;
  not on our ingenuity or lack thereof!

Security…

- Security based only on the validity of laws of nature;
  not on our ingenuity or lack thereof!

- Devices are have been built, that transmit random keys securely over 100 km of optical fibre

Id3000 by IDQuantique, Switzerland

Security…

- Security based only on the validity of laws of nature;
  not on our ingenuity or lack thereof!

- Devices are have been built, that transmit random keys securely over 100 km of optical fibre

Id3000 by IDQuantique, Switzerland

- Prototypes at IQC (over fibre); and between IQC and PI over free space

What else?

Karpov ⟷ Kasparov

Phone line

- Who plays white?
- Coin-flipping:

  follow some randomized procedure such that
  - If both are honest, outcome is unbiased

Karpov ⟷ Kasparov

Phone line

- Who plays white?
- Coin-flipping:

  follow some randomized procedure such that
  - If both are honest, outcome is unbiased
  - If any one is dishonest and the other honest, outcome is heads or tails with probability at most ½.

    (the honest party may cry "foul")

A quantum proposal

- Karpov:

  Picks a random orientation a

  $a = 0 \leftrightarrow$ rectilinear $\quad a = 1 \leftrightarrow$ diagonal

Quantum protocol…

- Second step: Kasparov

  Picks a random bit b,

  sends bit to Karpov

- Third step: Karpov

  Reveals orientation a, and polarization φ

- Fourth step: Kasparov

  Checks if photon received is in claimed polarization. If not, cries "foul", and quits.

- Finally (no foul): both agree on outcome $a \oplus b$

With one dishonest player…

- Karpov:

  Once he sends a photon in a chosen polarization, he cannot change it

Security

Security

Secure if Kasparov tries to cheat, but...

...there is a subtle quantum strategy for Karpov:

1. Prepares a pair of photons with correlated polarization

$$(1/\sqrt{2}) \quad [\,(r_0, r_0) + (r_1, r_1)\,].$$

Sends one photon to Kasparov.

2. When $b = 0$, measures his photon in the rectilinear basis.
Claims $a = 0$, $\varphi =$ observed polarization

Bias of outcome

When $b = 1$…

$$(1/\sqrt{2}) \quad [\,(r_0, r_0) \;+\; (r_1, r_1)\,]$$

$$= (1/2\sqrt{2}) \quad [\,(d_0 - d_1, d_0 - d_1) \;+\; (d_0 + d_1, d_0 + d_1)]$$

Quantum coin-flipping

- This, and *all* other conceivable protocols are doomed to fail; ideal quantum coin-flipping is impossible

  (without computational assumptions)

Quantum coin-flipping

- This, and *all* other conceivable protocols are doomed to fail; ideal quantum coin-flipping is impossible

  (without computational assumptions)

- Relaxed versions are possible, though, where *no player* can force her favourite outcome with probability more than $\frac{1}{2} + \varepsilon$, for any $\varepsilon > 0$.

Quantum coin-flipping

- This, and *all* other conceivable protocols are doomed to fail; ideal quantum coin-flipping is impossible

  (without computational assumptions)

- Relaxed versions are possible, though, where *no player* can force her favourite outcome with probability more than $\frac{1}{2} + \varepsilon$, for any $\varepsilon > 0$.

Final remarks

Quantum coin-flipping

- This, and *all* other conceivable protocols are doomed to fail; ideal quantum coin-flipping is impossible

  (without computational assumptions)

- Relaxed versions are possible, though, where *no player* can force her favourite outcome with probability more than $\frac{1}{2} + \varepsilon$, for any $\varepsilon > 0$.

Final remarks

Final remarks

- Access to quantum mechanical systems enables new cryptographic protocols with strong security guarantees

Final remarks

- Access to quantum mechanical systems enables new cryptographic protocols with strong security guarantees

- Not all tasks are realizable

Final remarks

- Access to quantum mechanical systems enables new cryptographic protocols with strong security guarantees
- Not all tasks are realizable
- Development of new protocols important in light of quantum attacks on existing public-key systems