Secure ***Communications***

History of Cryptography

BSc in Information Security & Digital Forensics.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Core of Cryptography

The core of cryptography is **secure communication** that essentially consists of two parts:

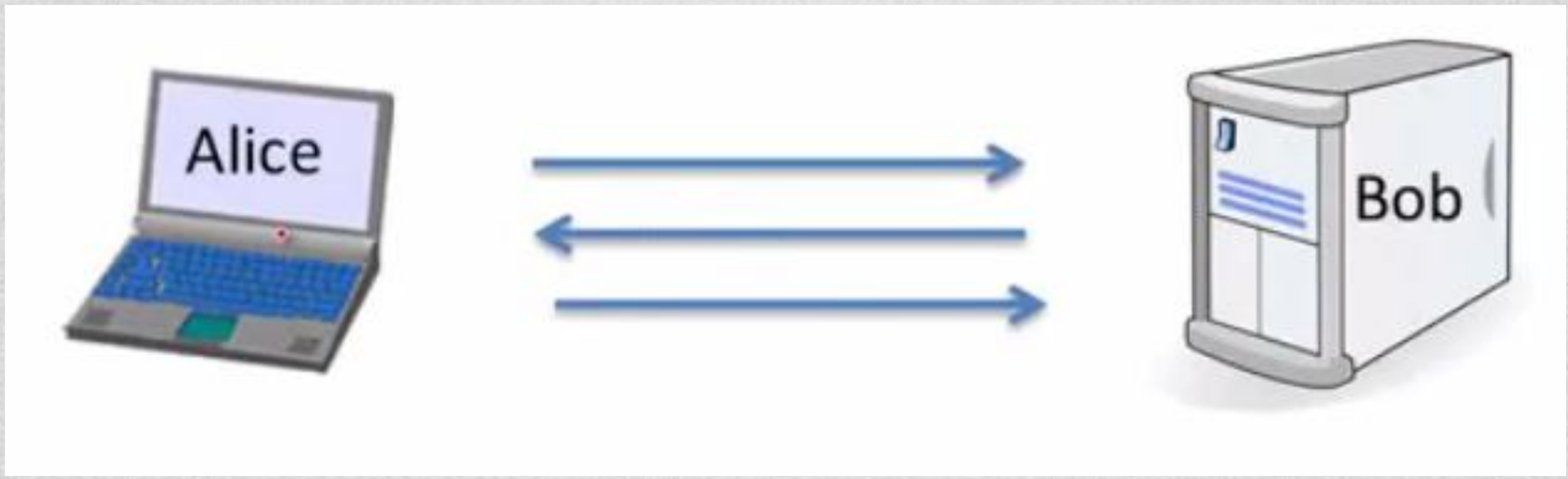
- **Secure key establishment**
- **Secure communication** (once we've managed key exchange)

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Core of Cryptography

Secured key establishment essentially amounts to **Alice** and **Bob** sending messages to one another such that at the end of this protocol, there's a shared key that they both agree on,

But a poor attacker who listens in on this conversation has no idea what the shared key is.



Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Core of Cryptography

We'll talk about **encryption schemes** that allow us to exchange messages in such a way that an attacker can't figure out what messages are being sent back and forth. And furthermore an attacker cannot even tamper with this traffic without being detected.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Cryptography can do so much more!

Our first example is what's called a **digital signature**. So a digital signature, basically, is the analog of the signature in the physical world.

Other uses of cryptography include **anonyomous communications** and even **anonymous digital cash.**

And cryptography can even be applied to **election protocols**.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

History of Cryptography

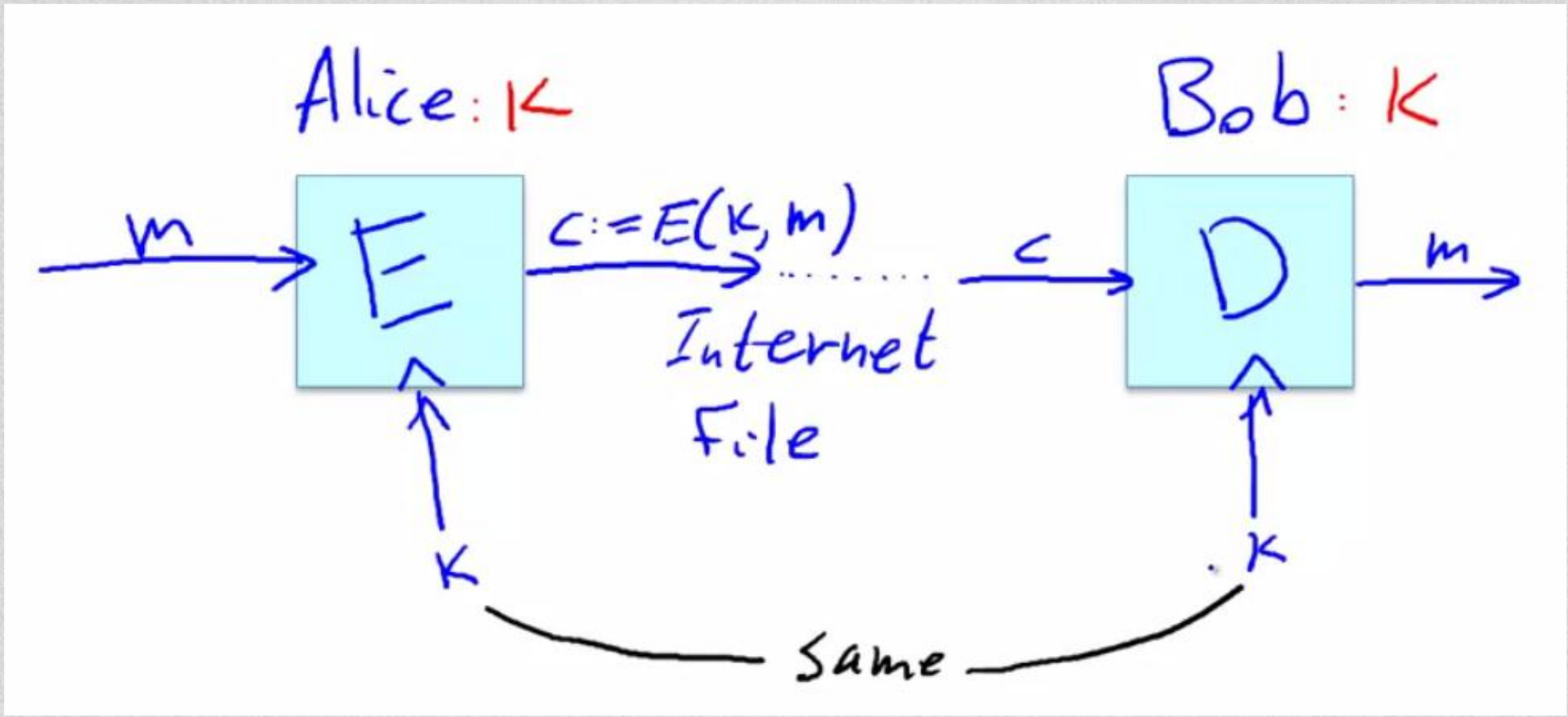
Before we start with the technical material, I want to tell you a little bit about the history of cryptography.

Here, I'm just going to give you a few examples of historical ciphers, all of which are badly broken.

So to talk about ciphers the first thing I'm going to do is introduce our friends **Alice** and **Bob**, who are trying to communicate securely and there is an **attacker** who's trying to eavesdrop on their conversation.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Symmetric Ciphers



Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Symmetric Ciphers

So to communicate securely, they're going to share a **secret key**, which I'll denote by **K**. They both know the secret key. But the attacker does not know anything about this key K.

Now they use a **cipher**, which is a pair of algorithms, an **encryption** algorithm denoted by **E**, and a **decryption** algorithm, **D**.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Symmetric Ciphers

These algorithms work as follows:

the encryption algorithm **E** takes the **message M** as inputs. And it takes as inputs, the **key K**. And then it outputs a **ciphertext**.

Now the ciphertext is transmitted over the internet to Bob, somehow. When the ciphertext reaches Bob, he can plug it into the decryption algorithm and give the decryption algorithm the **same key** K.

The decryption algorithm then outputs the original **plaintext** message..

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

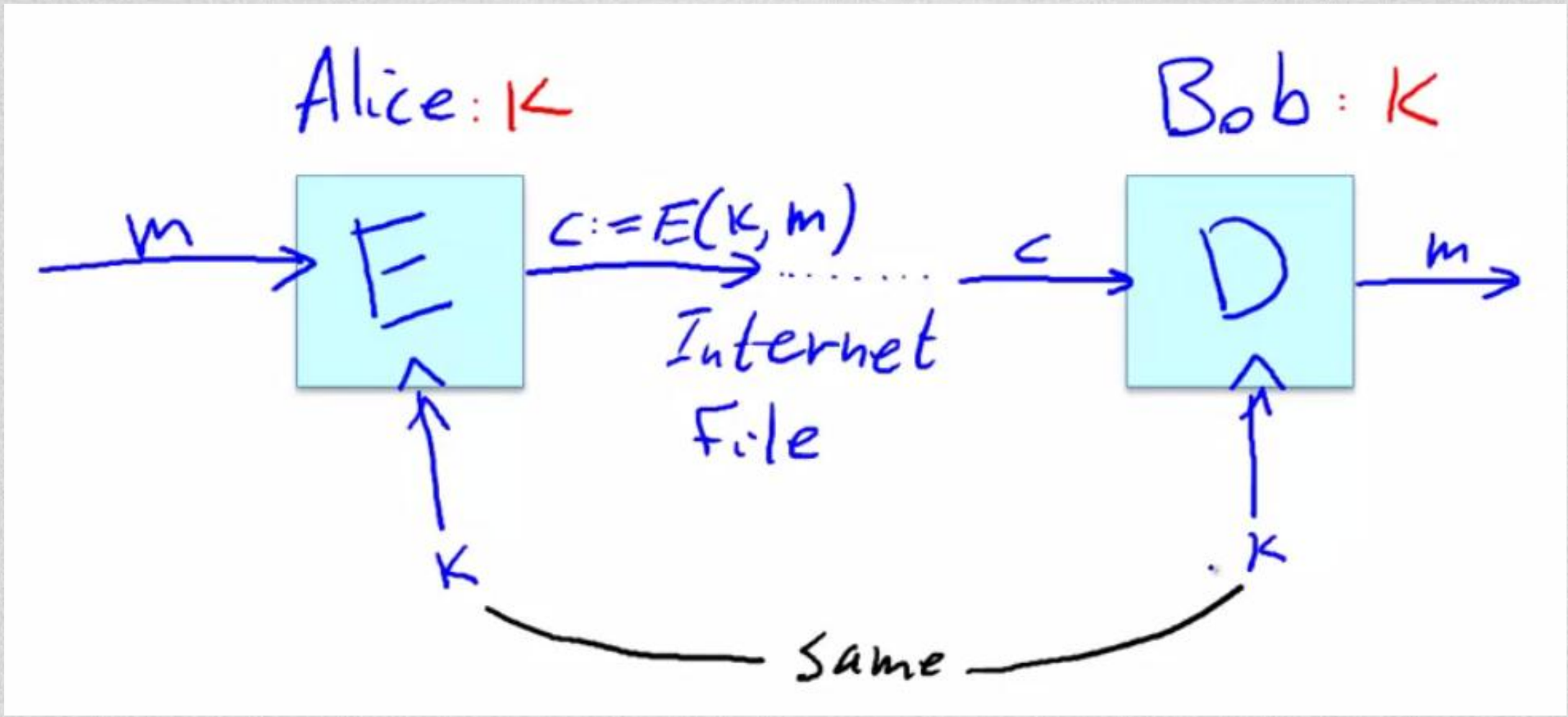
Symmetric Ciphers

Now the reason we say that these are symmetric ciphers is that both the **encrypter** and **decrypter** actually use the same key K.

As we'll see later in the course, there are ciphers where the encrypter uses one key and the decrypter uses a different key.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Symmetric Ciphers



Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Historic Examples (All badly broken)

1. **Rotational ciphers** (Caesar, Rot13, Rot 47,)
2. **Subsitution cipher** (how big is the **key space**?)
3. **Vigener cipher**
4. **Rotor machines** (theHibber, Enigma)
5. **DES**

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Try break these Examples (Encodings not cryptography)

1. 01000001 00100000 01110011 01101001 01101101 01110000 01101100 01100101 00100000 01000010 01101001 01101110 01100001 01110010 01111001 00100000 01100101 01101110 01100011 01101111 01100100 01101001 01101110 01100111

2. 54 68 69 73 20 6f 6e 65 20 69 73 20 68 65 78 2c 20 6e 6f 74 20 74 68 65 20 6c 69 6d 69 74 65 64 20 63 68 61 72 61 63 74 65 72 20 73 65 74

3. 70 105 110 97 108 108 121 32 97 110 32 97 115 99 105 105 32 101 110 99 111 100 101 100 32 109 101 115 115 97 103 101

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Try break these Examples (simple ciphers)

4. RQH RI WKH HDUOLHVW IRUPV RI KLGGHQ PHVVDJHV

5. n fvzcyr ebg13 rapbqvat

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Thank You !

End of Section

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie