

# The History of Cryptography and Codes

---

*19<sup>th</sup> May 2018, Birkbeck*

Thank you for participating in this conference on the History of Cryptography and Codes. It has been organised by the British Society for the History of Mathematics (BSHM), with support from the Department of Economics, Mathematics and Statistics at Birkbeck College, University of London. Our Birkbeck events are now a regular fixture in the BSHM calendar and one of our most popular annual events. It has been a while since we have had an event focused on the cryptography and coding, and 2018 seemed a good year to do it, as it is the 70<sup>th</sup> anniversary of Claude Shannon's influential 1948 paper "A Mathematical Theory of Communication", which essentially founded information theory, for example introducing the term "bit" for a unit of information. We have an exciting programme for the day with six excellent speakers covering a range of topics from the origins of cryptography through to the modern day. We hope you enjoy it. If you are not already a member of the BSHM, we encourage you to consider joining. You can go to the website [www.bshm.ac.uk](http://www.bshm.ac.uk) for more information.

## On Arrival

- The conference will be in the Clore building (building number 2 on the map on page 5). Note, this is a different location from previous years; the Clore building is opposite the main Birkbeck building where previous years' conferences have been held. For journey planning, the postcode is WC1E 7HX. Nearby stations include Euston, Russell Square and Warren Street.
- Registration and all tea/coffee breaks through the day will be in the basement foyer; on entering the Clore building just turn right and head down the stairs; there is also lift access if required. It will be clearly signposted.
- All lectures will be in the basement lecture theatre of the Clore building adjacent to the tea/coffee and registration area.
- The full programme with abstracts is on pages 2 and 3.
- To keep registration fees to a minimum, lunch is **not** provided. There are numerous cafes, restaurants and shops nearby; a few suggestions are given on page 4.

## Programme

### 9:30 Registration and Coffee/Tea

### 10.00 Opening remarks

#### 10.10 Dr Elizabeth Quaglia (Royal Holloway, University of London)

##### *Secrecy as an art - A journey through classical cryptography*

In this talk, we will explore the history of secret messaging from its inception up to the modern era of cryptography, when secrecy evolved from art to science. In a journey through space and time, we will uncover the reasons behind the need for cryptography, and we will describe some of the most influential historical ciphers, as well as the techniques that broke them.

#### 10:55 Klaus Schmeh (Journalist, Blogger ([www.schmeh.org](http://www.schmeh.org)), Author)

##### *Solving Historical Ciphers with Modern Means*

Many old encryption methods are still hard to break today. For instance, cryptanalyzing a Turning Grill (a cipher device already known in the 18th century) is far from trivial. Many other encryption methods of historical importance can nowadays be broken, for instance Enigma messages from WW2, ADFGVX-ciphertexts from WW1, bigram substitutions, cipher slide messages, and double column transpositions. This presentation will introduce a number of non-trivial ciphers that played an important role in history and explain how they can be broken with modern means. This will be demonstrated with original ciphertexts from past centuries, some of which were deciphered only recently. A number of interesting improvements in this area have been developed in recent years. Research is still going on. In spite of all these efforts, there are still surprisingly many historical encryption methods (and original ciphertexts) that are unbroken to date. Among others, Enigma messages with less than 70 letters, double column transpositions with long key words, and numerous cold war ciphers still baffle cryptanalysts. However, research goes on and we might see further improvements in the near future.

### 11.40 Tea/Coffee

#### 12:10 Sir John Dermot Turing

##### *The Codebreakers of Bletchley Park*

The success of the British codebreakers is widely praised but what impact did they actually have on the war? This talk will explain that many of the ideas about what Bletchley Park did are fundamentally wrong and describe both the process by which the two main German ciphers were broken and what the full impact of that was on the war.

Sir John Dermot Turing is the nephew and biographer of Alan Turing. He serves on the Bletchley Park Board and is a member of the Bletchley Park Trust's Historical Advisory Group.

**12:55 – 14:15 Lunch**

(See page 4 for lunch suggestions.)

**14:15 Professor Janos Körner (Sapienza University of Rome)**

*Claude Shannon in, and beyond, Information Theory*

Mathematics is one but its different parts use a different intuition. One does and understands mathematics at an intuitive level. Shannon built up Information Theory single-handedly using his brilliant and revolutionary intuition. It took a decade for his first students at MIT to translate his ideas, his definitions and theorems into precise mathematical statements with proofs. Shannon's theory sets precise theoretical limits to what is feasible in telecommunication. Yet his mathematical concepts go far beyond his engineering discipline and provide valuable tools in various parts of mathematics. We will illustrate this in combinatorics.

**15:00 Professor Keith Martin (Royal Holloway, University of London)**

*From Bletchley Park to the Everyday*

Since the Second World War, cryptography has evolved from an obscure technology used to protect wartime communications into an essential everyday technology. We chart some of the main developments along this journey, both technical and political. We will also cast an eye towards what the future might hold for cryptography.

**15:45 Coffee/Tea****16:15 Clifford Cocks CB FRS (Heilbronn Institute and Visiting Professor, King's College London)**

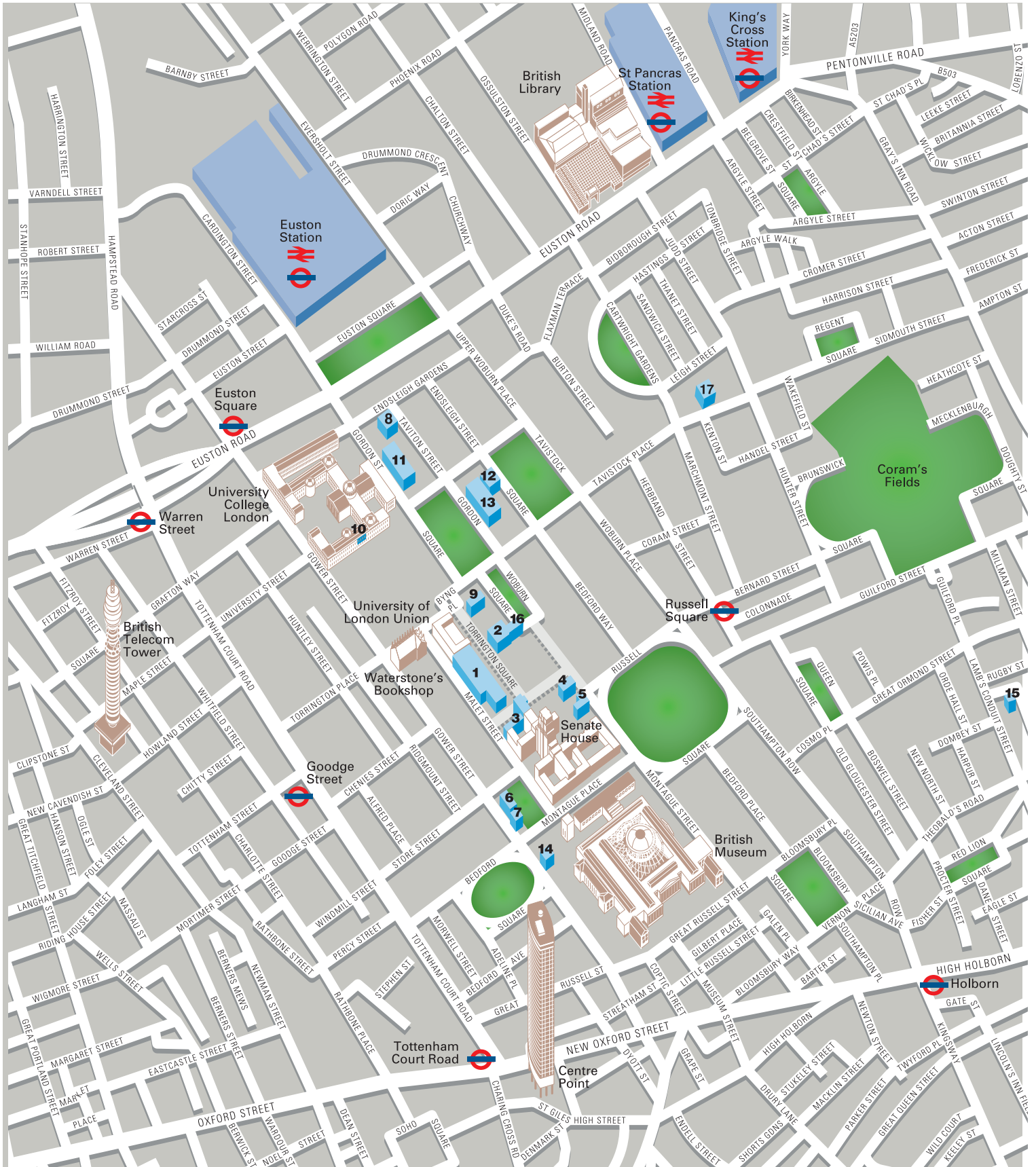
*The Discovery of Public Key Cryptography*





Public key cryptography is now ubiquitous and a critical component of online security. There were two parallel discoveries of this approach to cryptography during the 1970s, one in secret at Government Communications Headquarters in the UK, and the second, later discovery in academia in the USA. The talk will explain what public key cryptography is and then describe the discovery process, drawing out the similarities and differences between the two tracks.

**17:00 Close**

## Places to Eat near Birkbeck

- We have **an hour and twenty minutes** for lunch.
- Within Birkbeck (building 1 on the map), on the ground floor by the foyer, there is a **Costa Coffee** open from 9am which has a range of sandwiches, hot paninis and snacks.
- The **Birkbeck Student Union Shop** (Room B28) is located in the basement of the main building, below the foyer, and is open from 11am – 5pm on Saturdays. It sells hot beverages, sandwiches, wraps, bagels, confectionary and snacks.
- Externally there are several shops where you can buy sandwiches and snacks - you can bring these back and have them in the Clore building if you wish. The nearest are the Paradise Deli and the Co-op Local on **Store Street**, (South-West of Birkbeck on the map here <http://www.bbk.ac.uk/downloads/centrallondon.pdf>) or the Pret-a-Manger and Tesco Metro opposite Russell Square Tube. Store Street and Russell Square are marked on the map.
- The **Marlborough Arms** (36 Torrington Place – turn right out of the Clore building, then head left along Torrington Place, passing Waterstones on your left) is the nearest pub; it serves standard pub food. The **College Arms** on Store Street is an alternative. It's also where we will likely go for a post-conference drink.
- **Planet Organic** on Torrington Place (turn right out of the Clore building, then head left along Torrington Place, passing Waterstones and the Marlborough Arms on your left, and crossing Gower Street) sells vegetarian and vegan food to eat in or take away.
- **Olivelli** on Store Street has a cheapish set lunch.
- The **Russell Square Café** in Russell Square is also reasonable and close at hand.



-  Birkbeck buildings
-  Stations (rail/tube)
-  Stations (tube)
-  Major landmarks and other buildings of interest

- 1 Birkbeck main building, Torrington Square
- 2 Clore Management Centre
- 3 Senate House (North Block)
- 4 25-26 Russell Square
- 5 30 Russell Square
- 6 10-16 Gower Street
- 7 4 Gower Street
- 8 Evening Nursery
- 9 32 Torrington Square
- 10 South Wing UCL (access via Gower Street)
- 11 Gordon House
- 12 32 Tavistock Square
- 13 39-47 Gordon Square
- 14 7 Bedford Square

- 15 Knowledge Lab, 23-29 Emerald Street
- 16 The Wolfson Institute for Brain Development and Function in the Henry Wellcome Building
- 17 Egmont House

