# JAMES BOND'S MOST SECRET WEAPON

**Prof. Franck Leprevost**

Before creating James Bond in 1952, Ian Fleming (1908-1964) conducted intelligence activities for the UK. During WW2, among other things, he initiated the so-called "Operation Ruthless", a plan aiming to obtain the Enigma codes used by the German Navy. The plan was never implemented, much to the annoyance of Alan Turing, who was at that time heading the cipher school at Bletchley Park. Nowadays it is known that the efforts made by the team of mathematicians at Bletchley Park to break Enigma saved numerous lives, and probably shorten the war. Since this dramatic period, security of communications has known a huge development, even a kind of "revolution" in the mid 1970's. If during thousands of years symmetric-key cryptography mainly dominated the way messages were safely exchanged, the mid-1970's saw the emergence of a new concept: Public-Key Cryptography. Cryptology progressively left the sphere of art to become a science. The security of public-key crypto-systems relies on the difficulty to solve mathematical problems. Nowadays, there are mainly $2$ problems used in this setting: the Integer Factorization Problem (IFP) and the Discrete Logarithm Problem (DLP) in well-chosen groups. In the mid-1980's, Koblitz and Miller (independently) proposed to use elliptic curves, and defined the Elliptic Curve Discrete Logarithm Problem (ECDLP). According to today's knowledge, ECDLP is algorithmically safer than the other public-key crypto-systems. The increasing importance of mathematics in secure communications {\it{a posteriori}} legitimates the provocative title of this hopefully beautifully illustrated and entertaining conference.

Dear audience: No need to know anything in mathematics, nor in cryptology. Trust 007.

Lecture co-financed by the European Union in scope of the European Social Fund

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

EUROPEAN UNION
EUROPEAN
SOCIAL FUND