

MANY CHEERFUL FACTS

presents

A Riddle Wrapped In a Mystery

a talk by Johanna Franklin

12:10 am - 1:00 on Wednesday, February 9th, in room
1015.

After World War One, Germany adopted the Enigma machine as a primary component of its cryptosystem. When the Polish cipher bureau hired three young mathematicians to crack it, it marked the first time that mathematicians were recruited as cryptanalysts.

I plan to discuss the construction of an Enigma, demonstrate why the Germans believed it to be entirely secure and why they should not have, and explain how the Polish (and, later, the British) mathematicians exploited the Enigma's technical weaknesses and the Germans' careless use of it. No previous knowledge of cryptology is required.

*I am the very model of a modern Major General,
I've information vegetable, animal, and mineral,
I know the kings of England, and I quote the fights historical
From Marathon to Waterloo, in order categorical;
I'm very well acquainted, too, with matters mathematical,
I understand equations, both the simple and quadratical,
About binomial theorem I'm teeming with a lot o' news,
With many cheerful facts about the square of the hypotenuse!*

- Gilbert & Sullivan $P \circ P$