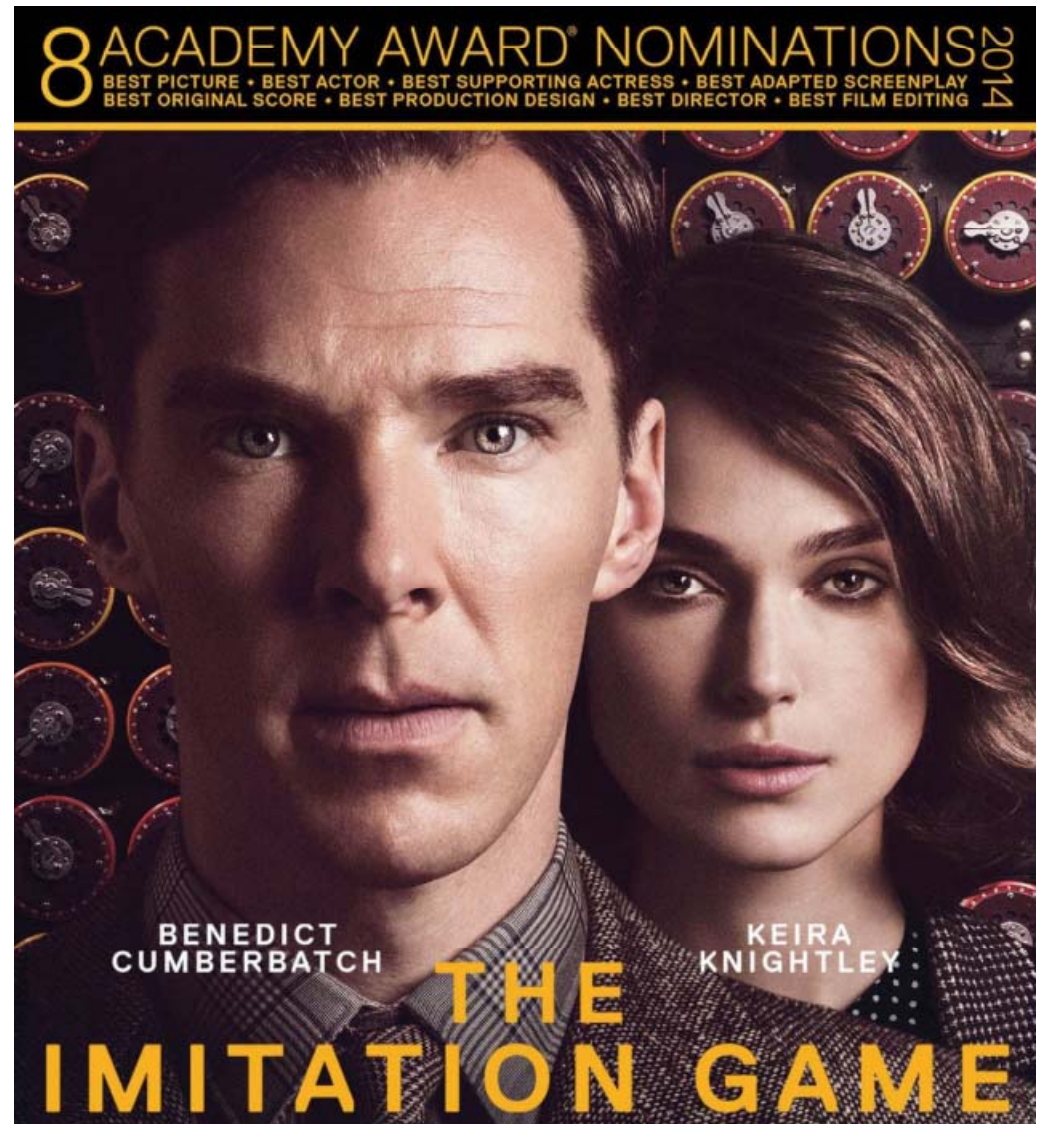


模仿遊戲

2014

班奈狄克·康柏拜區
綺拉·奈特莉



Enigma

恩尼格瑪

因為這個東西，
拍了好多部電影
獵殺 U571
攔截密碼戰

。 。 。

因為這個東西，
圖靈以及後續的
Keen完成自動
運算裝置Bombe
來協助破解

德軍了不起的對稱式加密裝置

因為這個東西同盟國死了很多很多人



- 1939 Alan Turing 沒有像電影裡製作那個機器他提出的是 **計算理論 (Computation Theory)** 以及 **圖靈機 (Turing Machine)** 運算模型
- 在計畫幾乎被軍方停下的時候, Turing 在酒吧裡聽到那個“女朋友”故事時, 徹夜想到的密碼破解方法 – 我們現在稱為 **Known Plaintext Attack (已知明文攻擊)**, 如果知道每天某一時間一定會送出來的密文所對應的明文, 破解相同鑰匙加密的密文的難度大幅度降低

- 為什麼電影叫做「**模仿遊戲**」？

這部商業電影裡真的沒有講清楚 !?

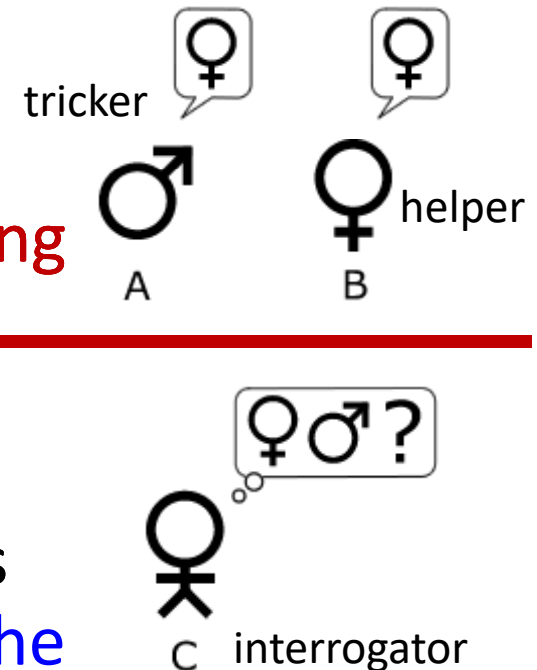
- Alan Turing 提出了一個 **判斷機器是
否具有智慧** 的方法 – **Turing Test** –
在人工智慧領域裡是很有趣的概念
- 這個方法的精神在 80 年代搖身一
變成為 **定義密碼系統安全性** 的基
本方法, 一直沿用到現在

Turing Test: Can machines think?

- 1950, Alan Turing, “Computing Machinery and Intelligence,” Mind LIX (236): 433–460
- Are there imaginable digital computers which would do well in the following

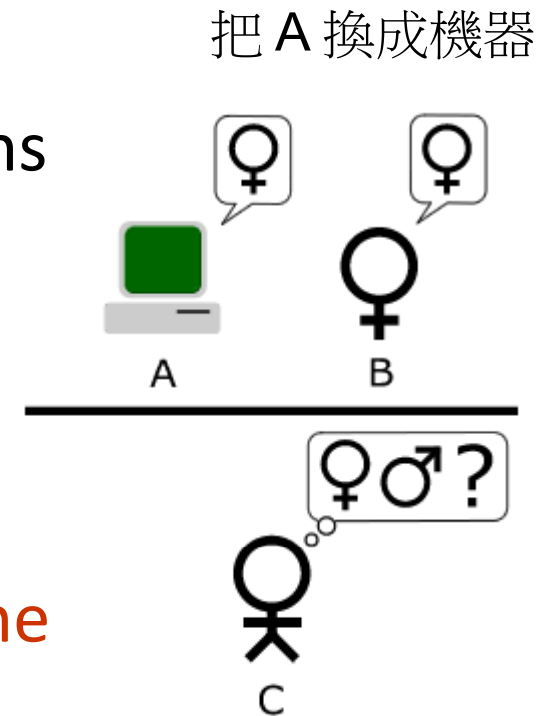
imitation game?

- the **interrogator C**, is given the task of **trying to determine whether player A is male while player B is female or the other way around**. Player A tries to trick C into making wrong decision. Player B attempts to assist C into making correct decision. **The interrogator only uses written questions and responses to make the decision.**



- The **interrogator C**, is given the task of trying to **determine which player – A or B – is the lying computer and which is an honest human**. The interrogator only uses the responses to written questions to make the decision.

- "If the interrogator decides wrongly as often when the game is played with the computer as he does when the game is played between a man and a woman", it may be argued that the **computer is intelligent**.



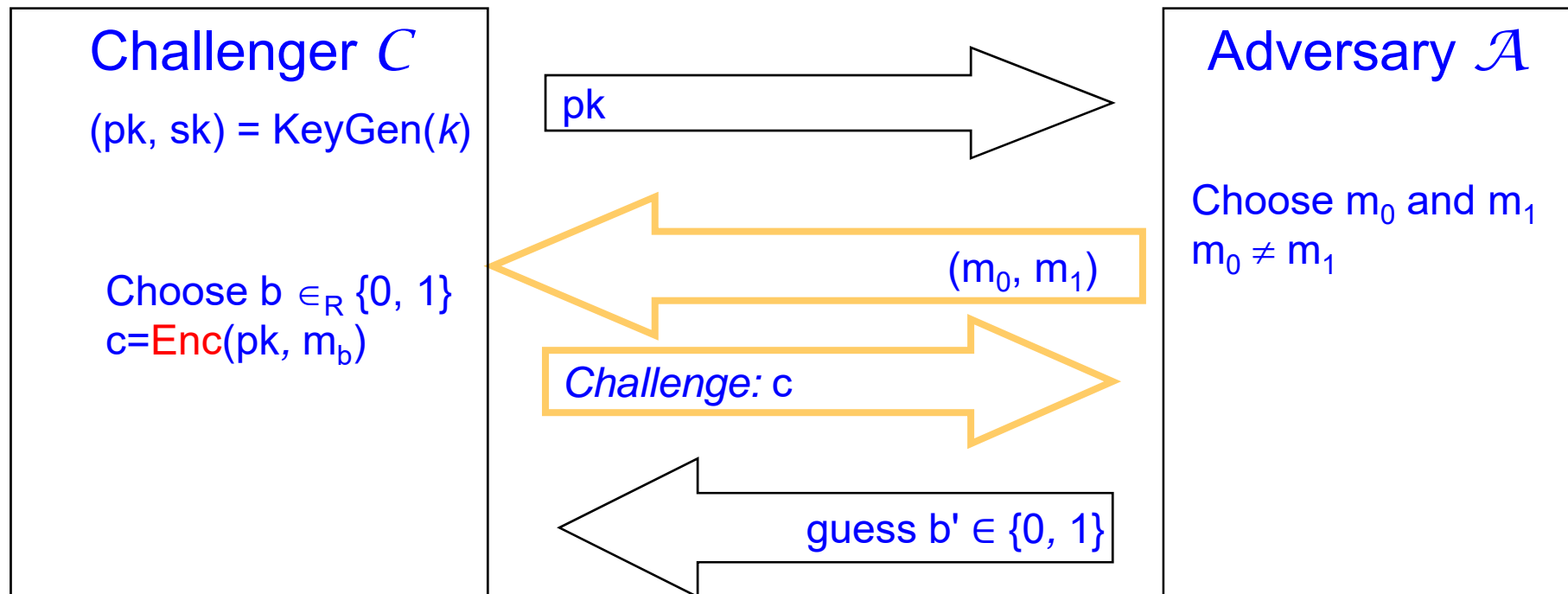
No machine is close to pass the test
for a very long time.

Finally, a machine is no longer a machine.

- On **7 June 2014**, 60th anniversary of Turing's death, a Turing test competition was held at the Royal Society London and was won by the Russian chatter bot **Eugene Goostman**. The bot, during a series of five-minute-long text conversations, convinced 33% of the contest's judges that it was human.
- The Turing test had been passed for the first time.

A Security Definition for $\text{Enc}(\cdot)$

- an **indistinguishability** game



\mathcal{A} wins the game if $b = b'$

$$\text{Adv}_{\mathcal{A}}(k) = \left| \Pr\{b=b'\} - \frac{1}{2} \right|$$

$\text{Enc}(\cdot)$ is secure if $\text{Adv}_{\mathcal{A}}(k)$ is negligible

不可分辨性