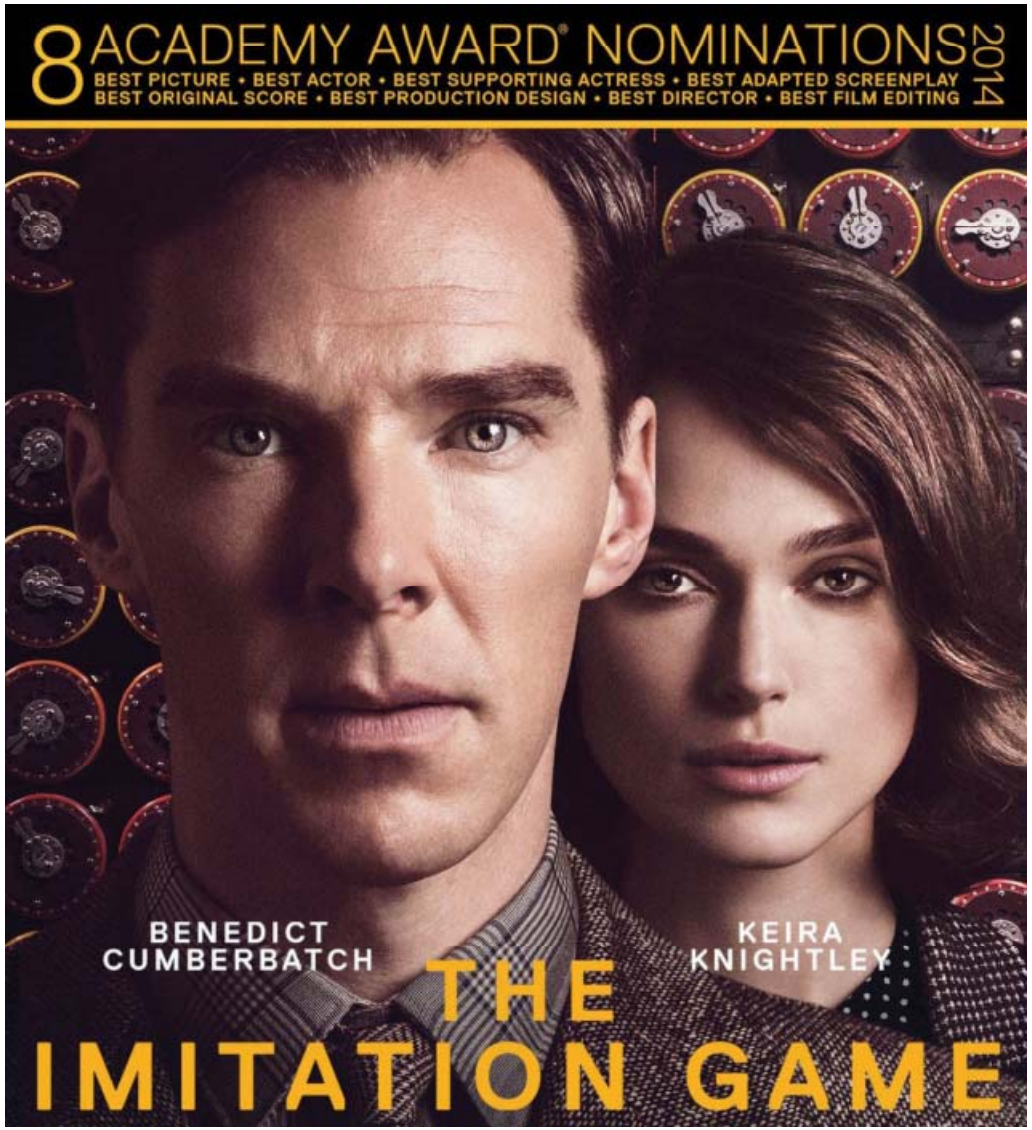
模仿遊戲

2014

班奈狄克·康柏拜區

綺拉·奈特莉



Enigma

恩尼格瑪

Enigma
恩尼格瑪

德軍了不起的對稱式加密裝置

Enigma
恩尼格瑪

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

Enigma
恩尼格瑪

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

因為這個東西,
拍了好多部電影
獵殺 U571
攔截密碼戰
。 。 。

Enigma
恩尼格瑪

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

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

- 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

- 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 (電影裡是 "Heil Hitler"), 破解相同鑰匙加密的密文的難度大幅度降低 (密鑰空間大幅縮小)

- 為什麼電影叫做「模仿遊戲」？

- 為什麼電影叫做「模仿遊戲」?

  電影裡好像沒有特別解釋什麼!?

- 為什麼電影叫做「模仿遊戲」?

  電影裡好像沒有特別解釋什麼 !?

  網路上很多附會的藝術層面解釋, 不過主角有說這是一個 Test, 也有邀請那個警探去 Play the game

- 為什麼電影叫做「模仿遊戲」?

  電影裡好像沒有特別解釋什麼 !?

  網路上很多附會的藝術層面解釋, 不過主角有說這是一個 Test, 也有邀請那個警探去 Play the game

  其實 Immitation game 是一種在 party 中常見的社交遊戲, 用來促進參與者的互動, 調節社交的氣氛 (沒什麼好說明的)

- 為什麼電影叫做「模仿遊戲」?

  電影裡好像沒有特別解釋什麼 !?

  網路上很多附會的藝術層面解釋, 不過主角有說這是一個 Test, 也有邀請那個警探去 Play the game

  其實 Immitation game 是一種在 party 中常見的社交遊戲, 用來促進參與者的互動, 調節社交的氣氛 (沒什麼好說明的)

  - Alan Turing 據此設計了一個 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

- 為什麼電影叫做「模仿遊戲」?

  電影裡好像沒有特別解釋什麼 !?

  網路上很多附會的藝術層面解釋, 不過主角有說這是一個 Test, 也有邀請那個警探去 Play the game

  其實 Immitation game 是一種在 party 中常見的社交遊戲, 用來促進參與者的互動, 調節社交的氣氛 (沒什麼好說明的)

  - Alan Turing 據此設計了一個 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?

Turing Test: Can machines think?

- **1950**, Alan Turing, "**Computing Machinery** and **Intelligence**," Mind LIX (236): 433–460

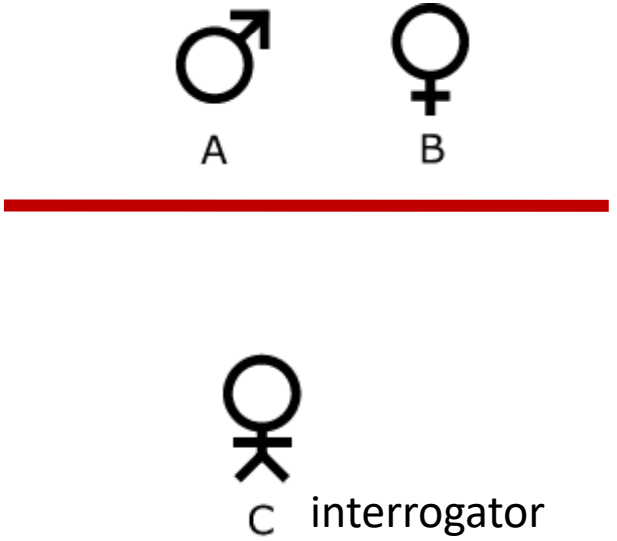
Turing Test: **Can machines think**?

- **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***?

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

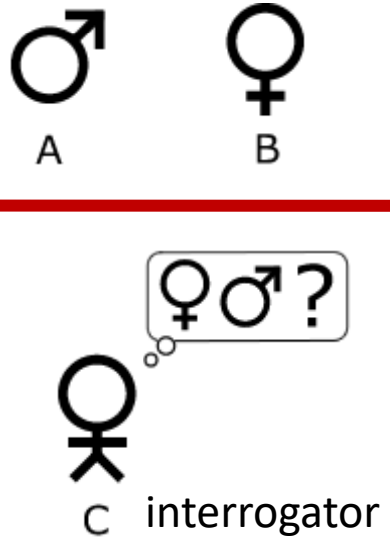
  imitation game?
- the **interrogator C**, is given the task



Turing Test: Can machines think?

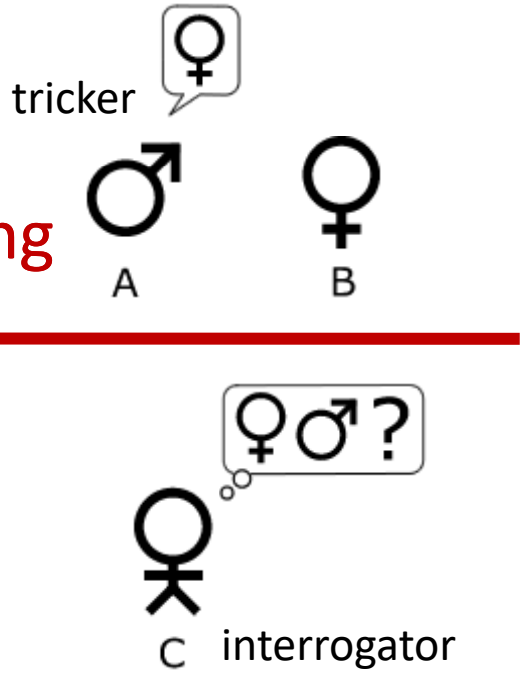
- **1950**, Alan Turing, "**Computing Machinery** and **Intelligence**," Mind LIX (236): 433–460
- Are there imaginable digital computers which would do well in the following

  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.



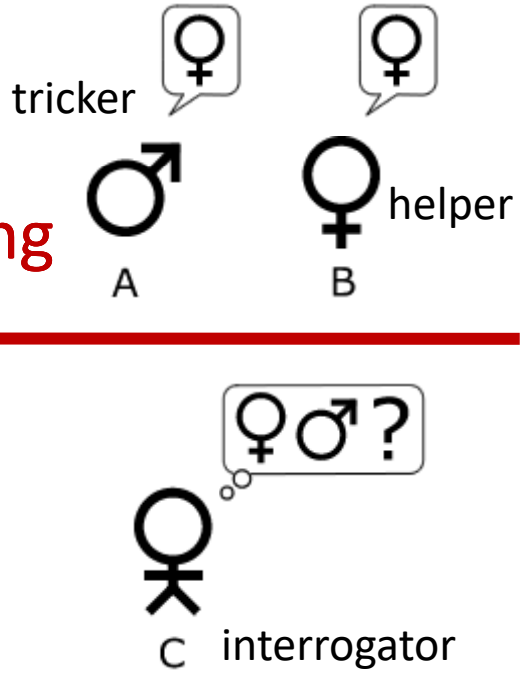
Turing Test: Can machines think?

- **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.



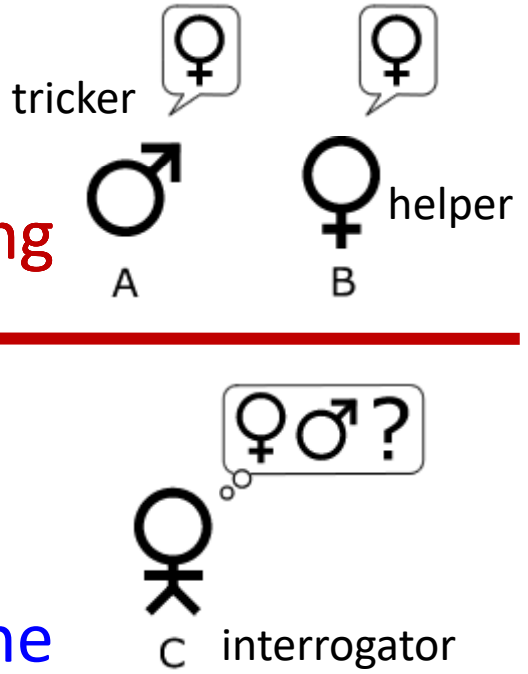
Turing Test: Can machines think?

- **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.

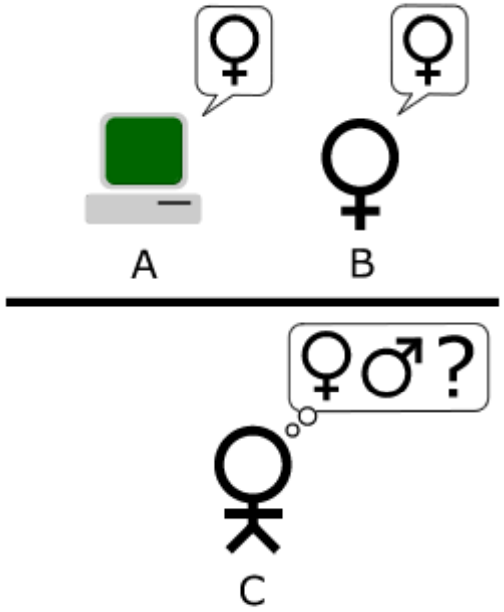


Turing Test: Can machines think?

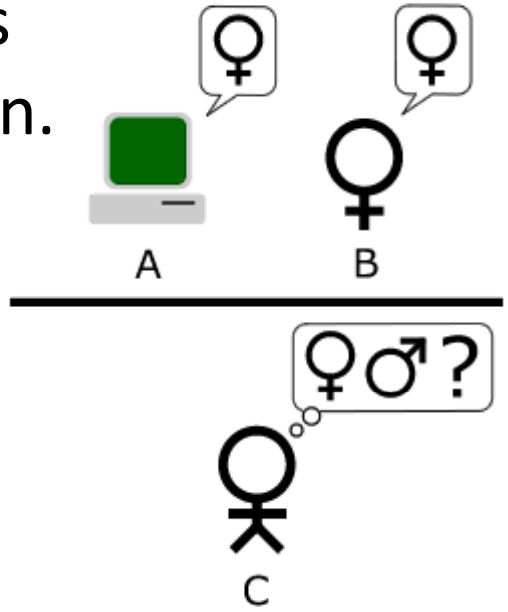
- **1950**, Alan Turing, "**Computing Machinery** and **Intelligence**," Mind LIX (236): 433–460
- Are there imaginable digital computers which would do well in the following ***imitation game***?
- the **interrogator C**, is given the task of trying to determine whether **player A** is male while **player 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.



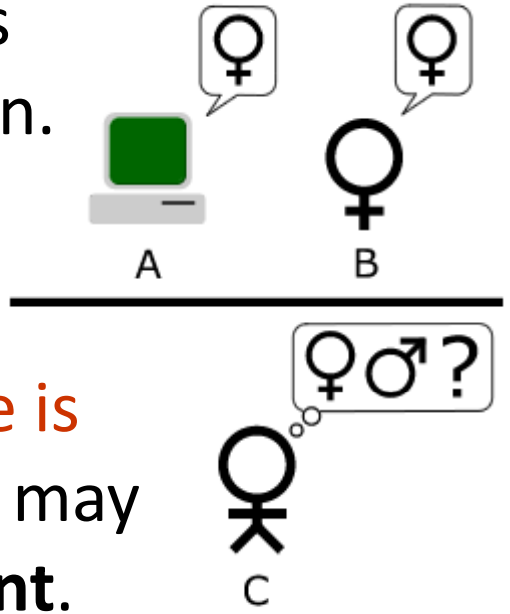
把 player A 換成機器



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

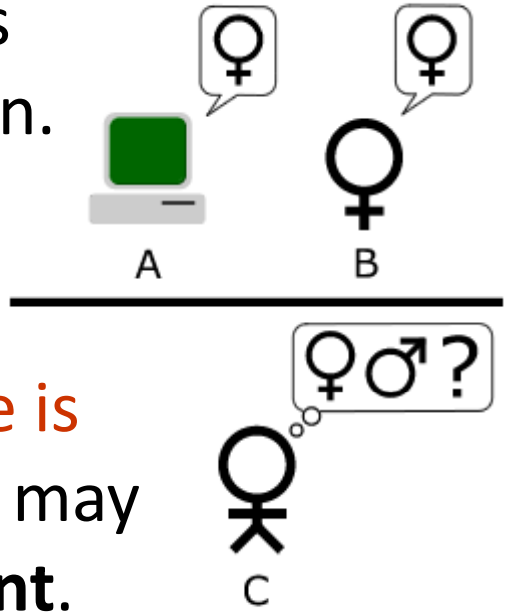


- The **interrogator C**, is given the same task of trying to determine whether **player A** is male while **player B** is female or the other way around. Player A still tries to trick C into making wrong decision. Player B attempts to assist C into making correct decision. The interrogator only uses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

- The **interrogator C**, is given the same task of trying to determine whether **player A** is male while **player B** is female or the other way around. Player A still tries to trick C into making wrong decision. Player B attempts to assist C into making correct decision.
  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**.
- The test results do **not** depend on the machine's ability to give **correct answers** to questions, only **how closely** its answers resemble those a human would give.

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

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

Finally, a machine is no longer a machine.

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

Finally, a machine is no longer a machine.

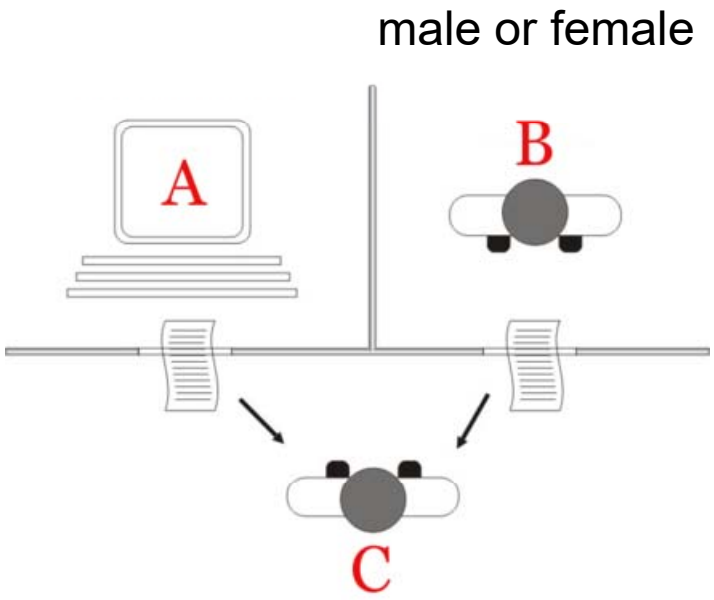
- On **7 June 2014**, 60th anniversary of Turing's death, a Turing test competition was held at the Royal Society London and was won by the Russian chatter bot **Eugene Goostman**. The bot, during a series of five-minute-long text conversations, convinced 33% of the contest's judges that it was human.

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

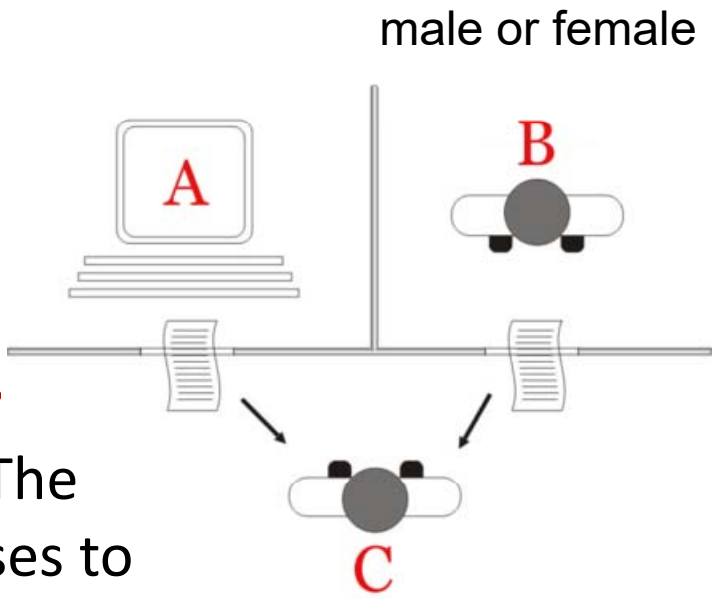
Finally, a machine is no longer a machine.

- 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.

Standard Interpretation – Another Version

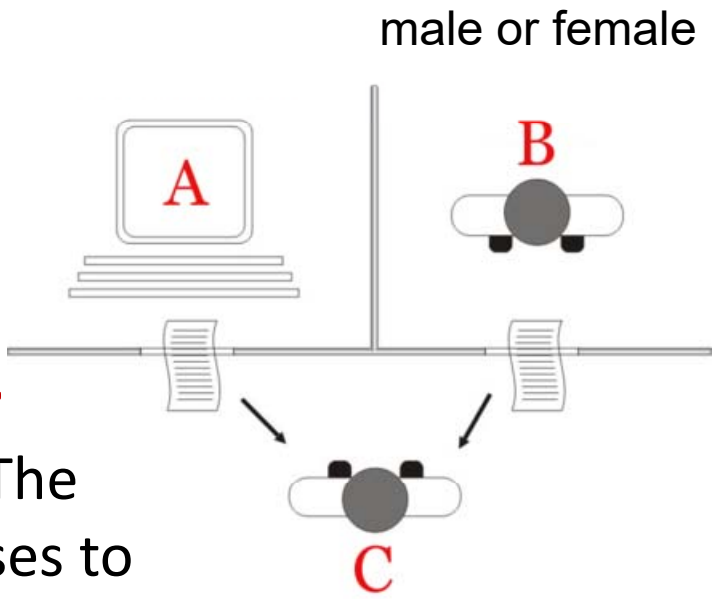


Standard Interpretation – Another Version



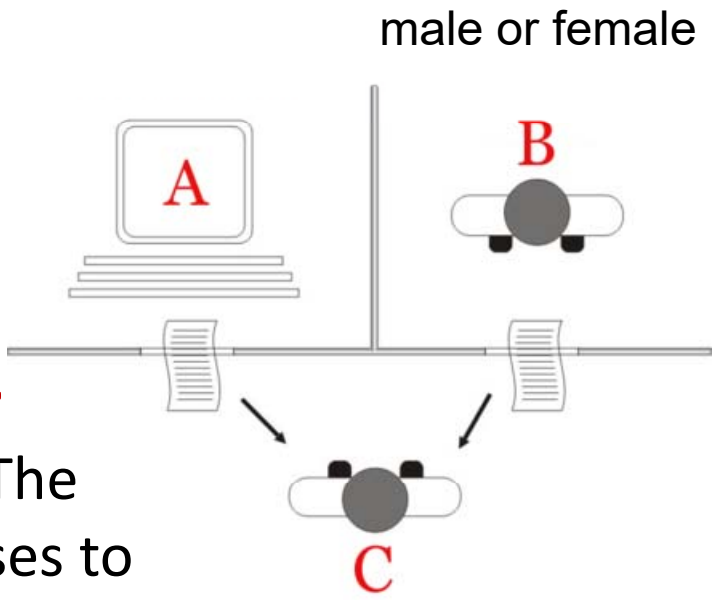
- Player C, the interrogator, is given the task of trying to determine **which player – A or B – is a computer and which is a human**. The interrogator is limited to using the responses to written questions to make the determination.

Standard Interpretation – Another Version



- Player C, the interrogator, is given the task of trying to determine **which player – A or B – is a computer and which is a human**. The interrogator is limited to using the responses to written questions to make the determination.
- Common understanding has it that the purpose of the purpose of the Turing test is not specifically to determine whether a computer is able to fool an interrogator into believing that it is a human, but rather whether a computer could imitate a human.

Standard Interpretation – Another Version



- Player C, the interrogator, is given the task of trying to determine **which player – A or B – is a computer and which is a human**. The interrogator is limited to using the responses to written questions to make the determination.
- Common understanding has it that the purpose of the purpose of the Turing test is not specifically to determine whether a computer is able to fool an interrogator into believing that it is a human, but rather whether a computer could imitate a human.
- While there is some debate regarding whether the "Standard Interpretation" is that described by Turing or, instead, based on a misreading of his paper, these versions are **not** regarded as **equivalent**, and their strengths and weaknesses are distinct.

A Security Definition for Enc(·)

A Security Definition for Enc(·)

- an indistinguishability game

A Security Definition for Enc(·)

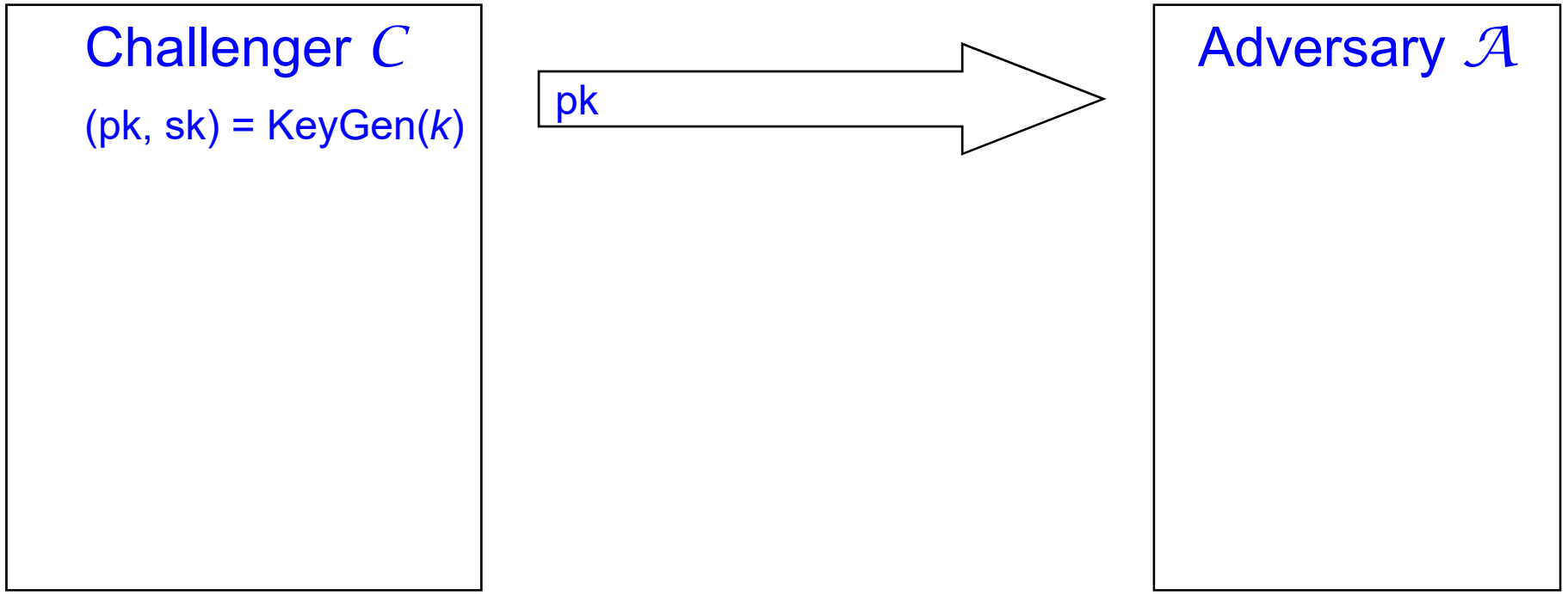
- an **indistinguishability** game

A Security Definition for Enc(·)

- an **indistinguishability** game

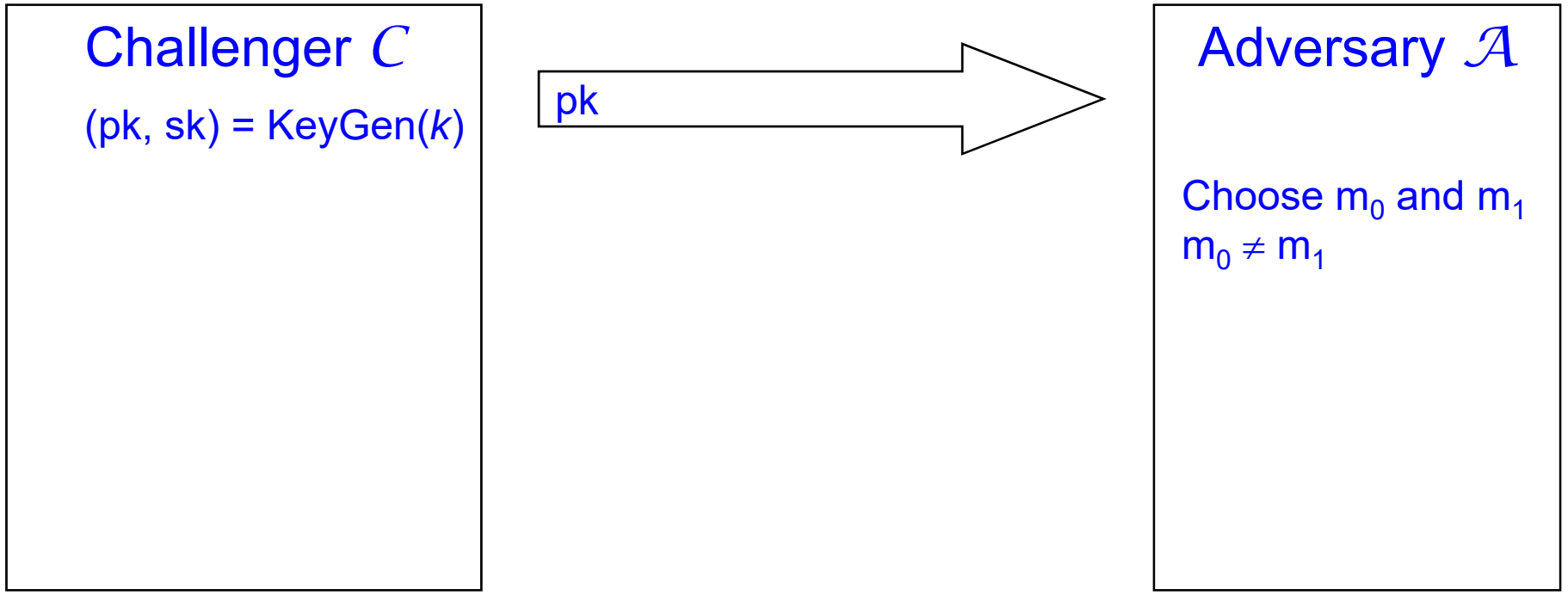
A Security Definition for Enc(·)

- an **indistinguishability** game



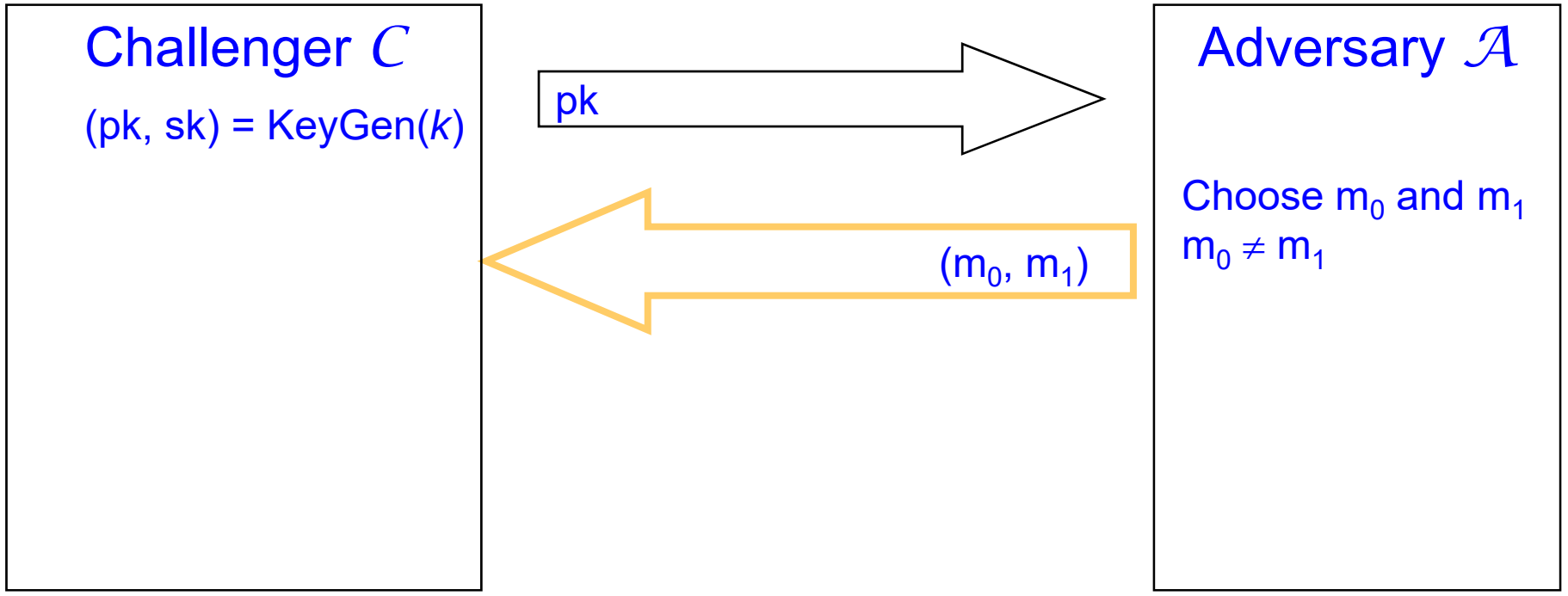
A Security Definition for Enc(·)

- an **indistinguishability** game



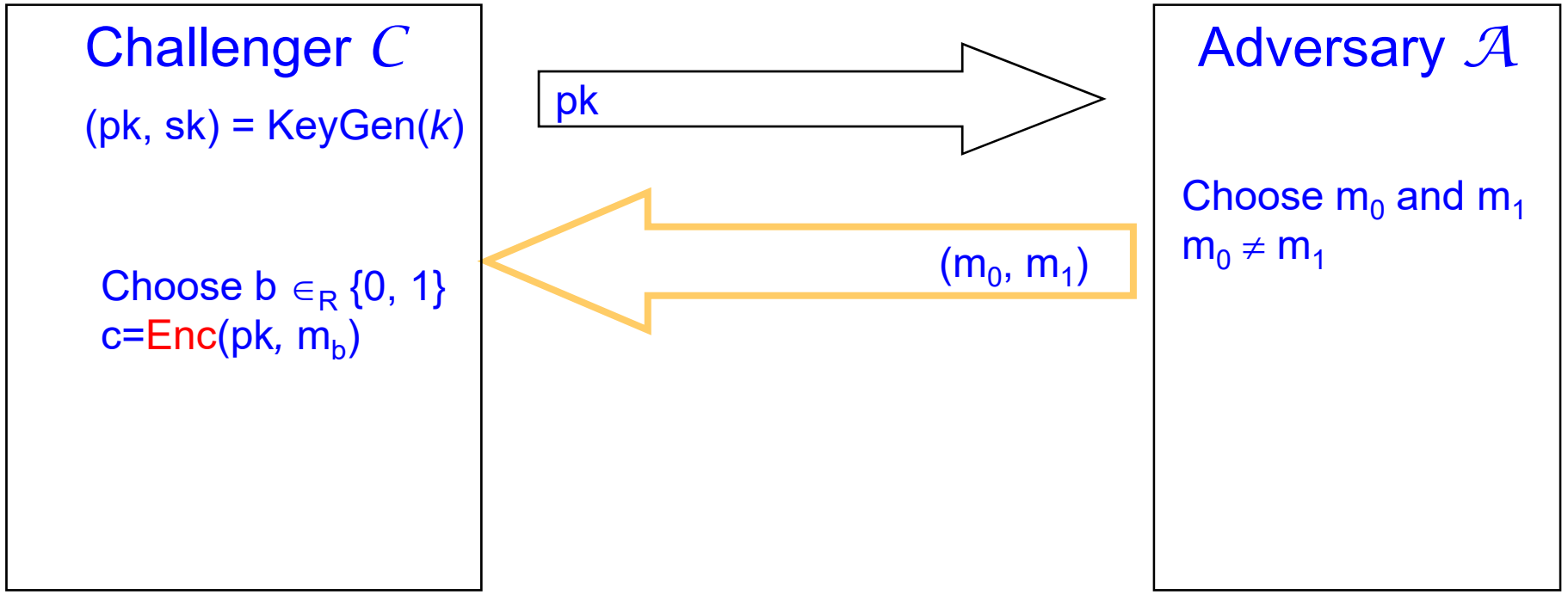
A Security Definition for Enc(·)

- an **indistinguishability** game



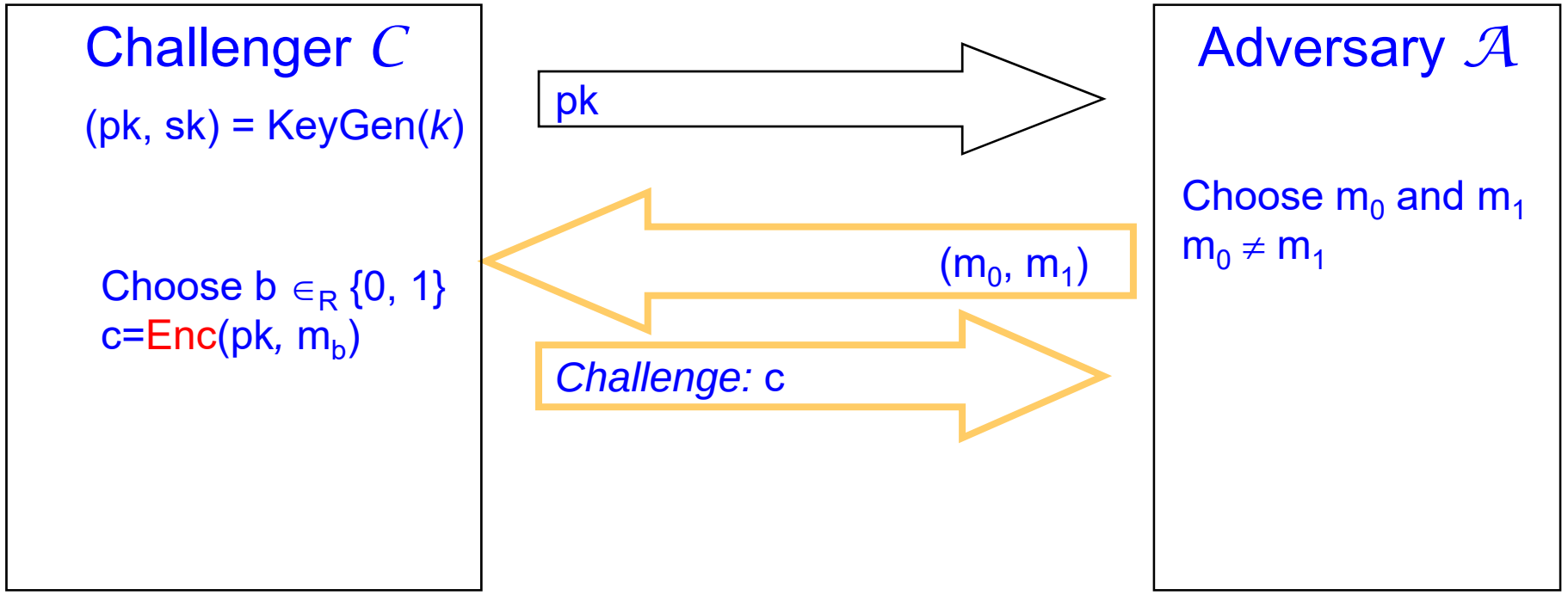
A Security Definition for Enc(·)

- an **indistinguishability** game



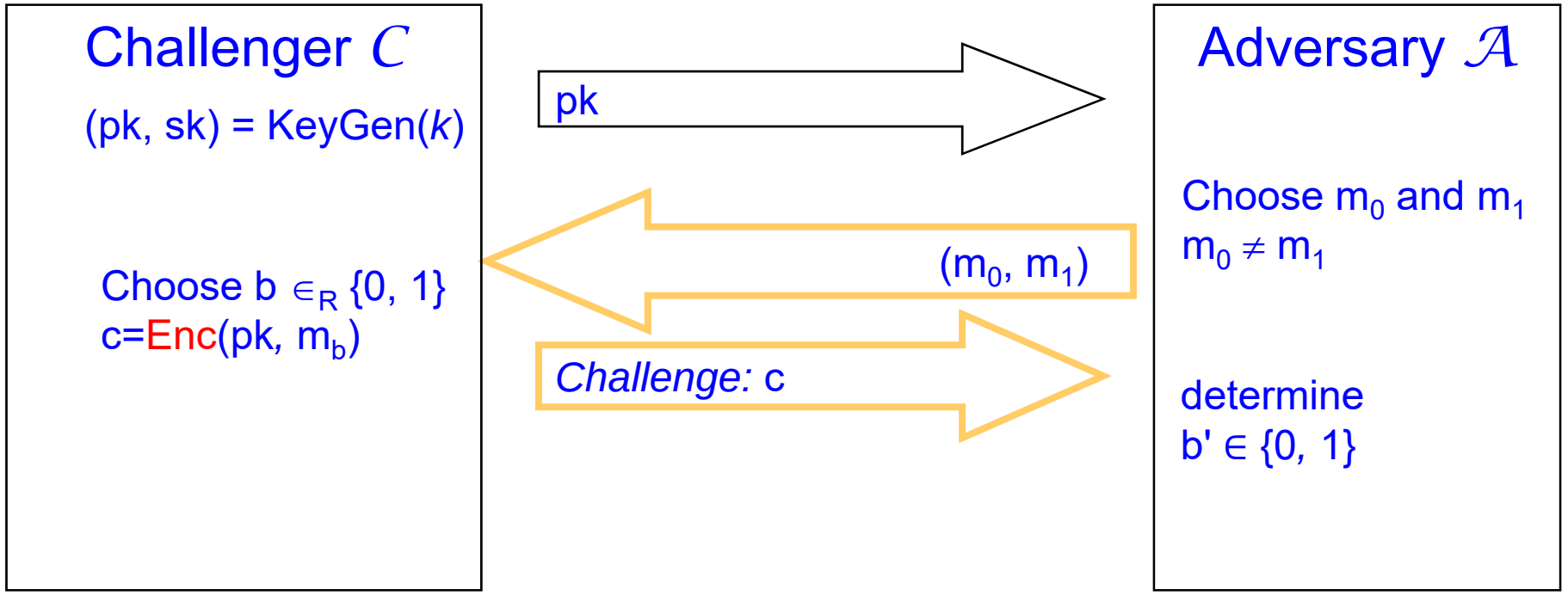
A Security Definition for Enc(·)

- an **indistinguishability** game



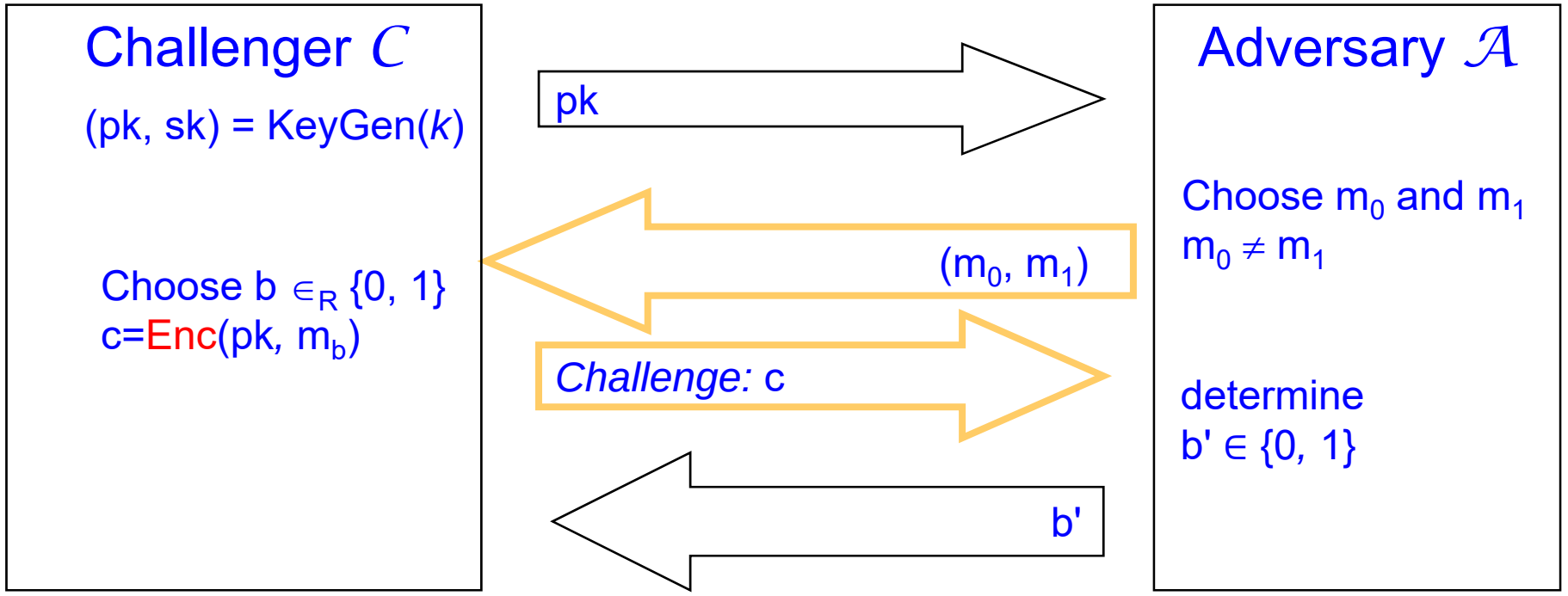
A Security Definition for Enc(·)

- an **indistinguishability** game



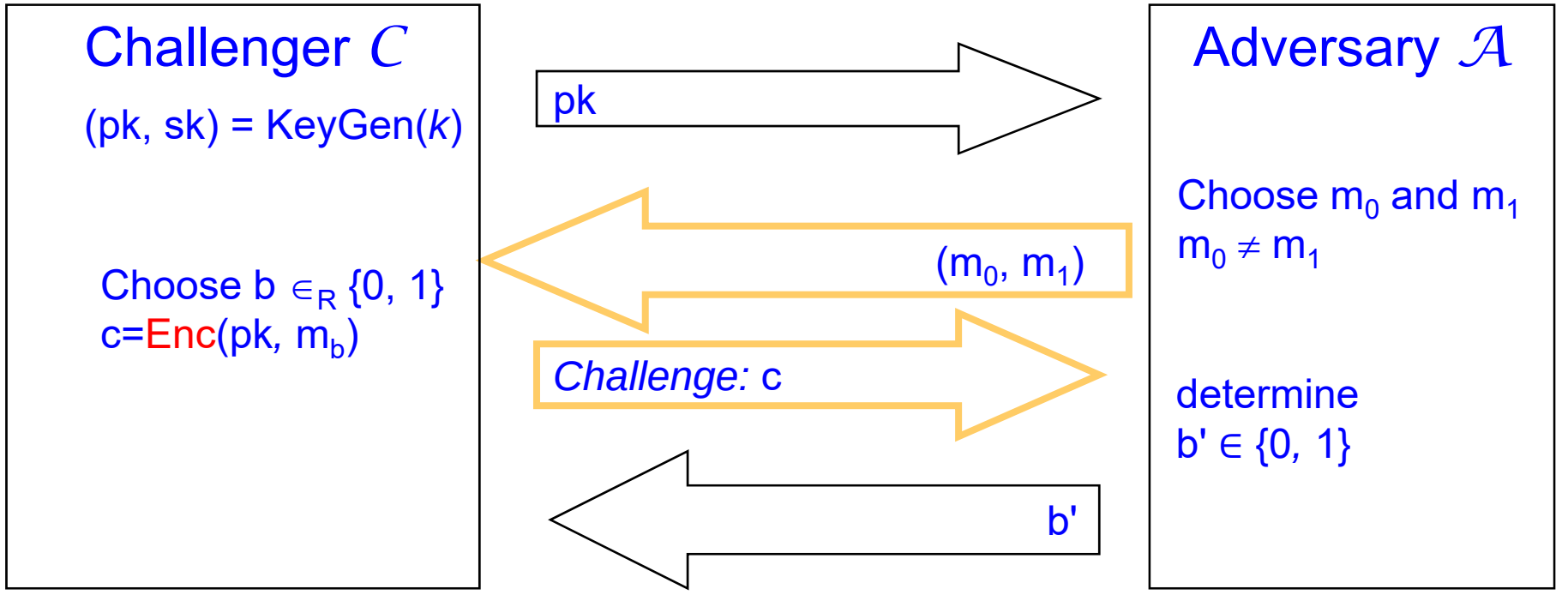
A Security Definition for Enc(·)

- an **indistinguishability** game



A Security Definition for Enc(·)

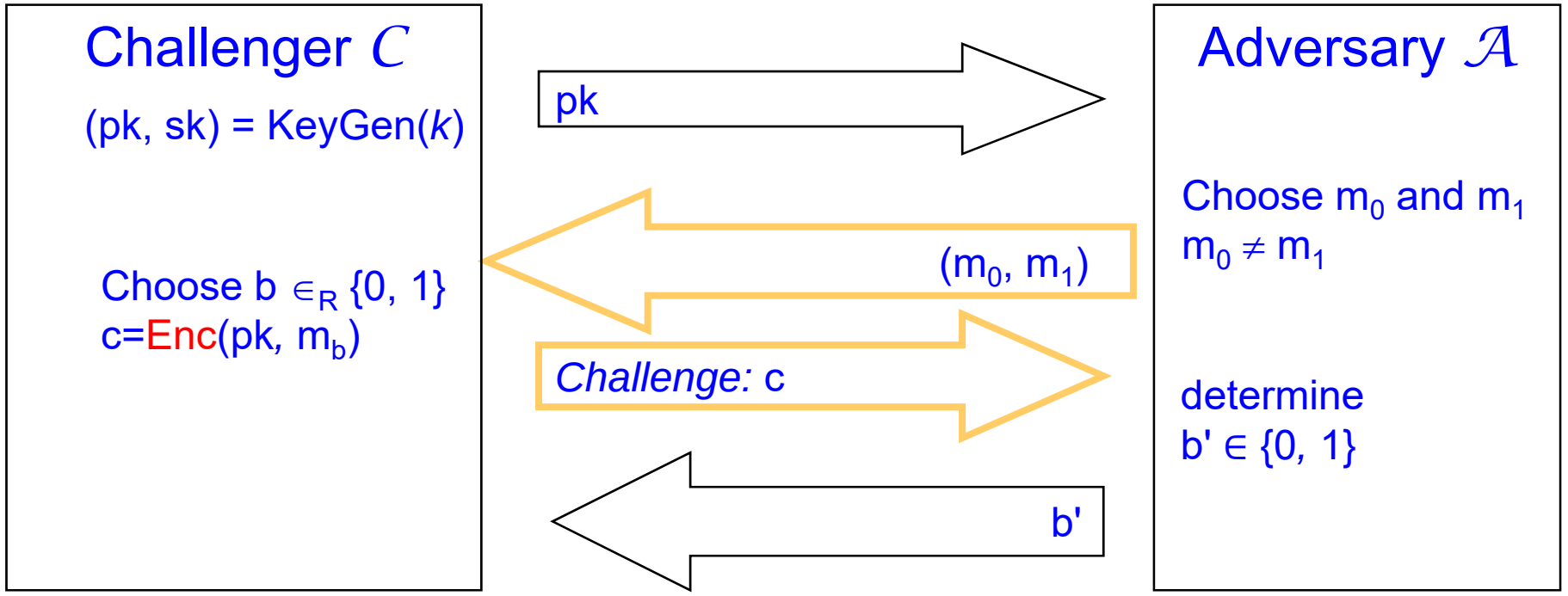
- an **indistinguishability** game



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

A Security Definition for Enc(·)

- an **indistinguishability** game

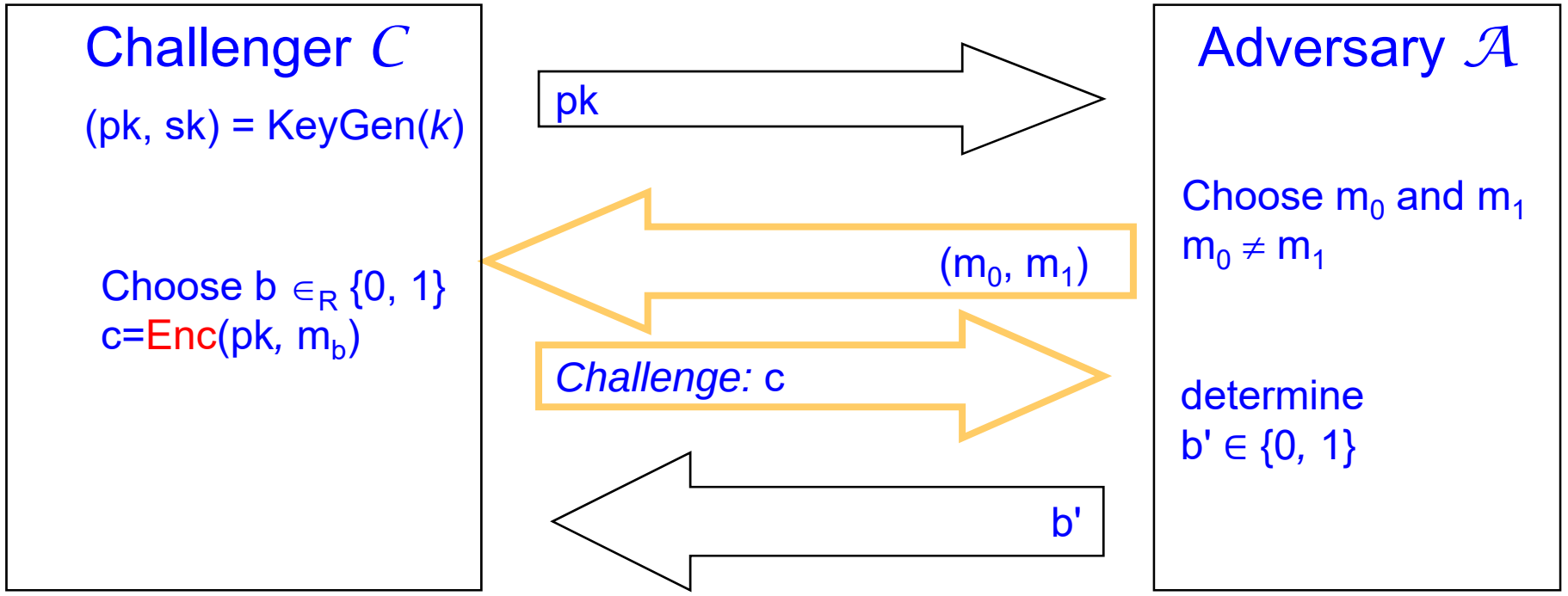


$\mathcal{A}$ wins the game if b = b'

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

A Security Definition for Enc(·)

- an **indistinguishability** game



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

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

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

不可分辨性

電影和事實不一致的地方

- 在 Bletchley Park 的機器叫 **Bombe** 不是 Christopher (可能是編劇用 圖靈 Alan Turing 中學時好友名字來得到戲劇效果)

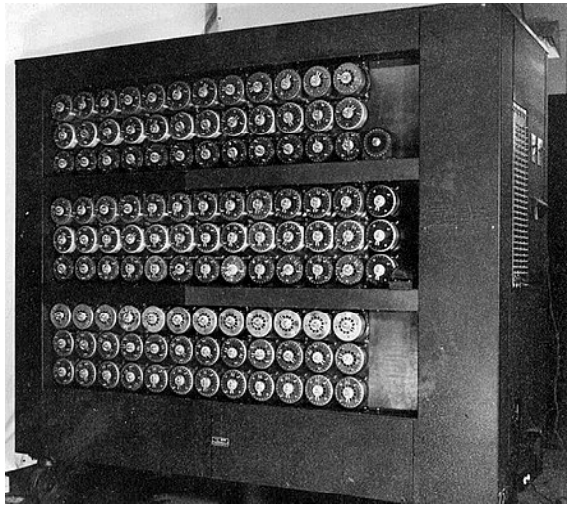
電影和事實不一致的地方

- 在 Bletchley Park 的機器叫 **Bombe** 不是 Christopher (可能是編劇用 圖靈 Alan Turing 中學時好友名字來得到戲劇效果)

http://en.wikipedia.org/wiki/Bombe

電影和事實不一致的地方

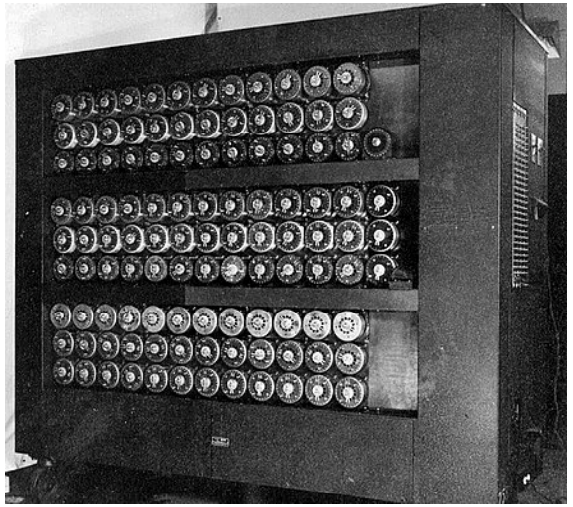
- 在 Bletchley Park 的機器叫 **Bombe** 不是 Christopher (可能是編劇用 圖靈 Alan Turing 中學時好友名字來得到戲劇效果)



http://en.wikipedia.org/wiki/Bombe

電影和事實不一致的地方

- 在 Bletchley Park 的機器叫 **Bombe** 不是 Christopher (可能是編劇用 圖靈 Alan Turing 中學時好友名字來得到戲劇效果)
- 圖靈沒有建造機器，圖靈在1939年提出的是「計算理論」，和理論設計思路，真正的機器是由 Harold Keen 和很多工程師完成的



http://en.wikipedia.org/wiki/Bombe

- 在整個破譯 Enigma Cipher 的初期工作中居功至偉的是波蘭密碼學家 Marian Rejewski, Jerzy Różycki 和 Henryk Zygalski，電影裡只是提了一下波蘭幫助走私了 Enigma Machine
  http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

- 在整個破譯 Enigma Cipher 的初期工作中居功至偉的是波蘭密碼學家 Marian Rejewski, Jerzy Różycki 和 Henryk Zygalski，電影裡只是提了一下波蘭幫助走私了 Enigma Machine
  http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma
- Bletchley Park Hut 6 最早在英倫空戰期間破譯了德國空軍的 Enigma，因為德國空軍對密碼疏於管理，讓 Bletchley Park 找到了很多人為漏洞來破譯密碼，其中就包括那個“女朋友”事件

- 在整個破譯 Enigma Cipher 的初期工作中居功至偉的是波蘭密碼學家 Marian Rejewski, Jerzy Różycki 和 Henryk Zygalski，電影裡只是提了一下波蘭幫助走私了 Enigma Machine
  http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

- Bletchley Park Hut 6 最早在英倫空戰期間破譯了德國空軍的 Enigma，因為德國空軍對密碼疏於管理，讓 Bletchley Park 找到了很多人為漏洞來破譯密碼，其中就包括那個“女朋友”事件
  - 電影裡所說德國電報員發送 CILLY 是根據真實事件改編的，這個事件發生在破譯德國空軍密碼工作中，德國空軍要求自己的電報員隨機選擇 3 個字母設置齒輪，再發送隨機選擇的 3 個字母幫助密文接受方將 Enigma 配置成相同設置來解碼。其中有個一個名為 **Wal**ter 的電報員，每天都將他的 Enigma 齒輪設置成他名字的前三個字母 W A L，然後發送的 3 個字母是他女朋友名字 **Kal**are 的前三個字母 K A L

- 在整個破譯 Enigma Cipher 的初期工作中居功至偉的是波蘭密碼學家 Marian Rejewski, Jerzy Różycki 和 Henryk Zygalski，電影裡只是提了一下波蘭幫助走私了 Enigma Machine
  http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

- Bletchley Park Hut 6 最早在英倫空戰期間破譯了德國空軍的 Enigma，因為德國空軍對密碼疏於管理，讓 Bletchley Park 找到了很多人為漏洞來破譯密碼，其中就包括那個“女朋友”事件
  - 電影裡所說德國電報員發送 CILLY 是根據真實事件改編的，這個事件發生在破譯德國空軍密碼工作中，德國空軍要求自己的電報員隨機選擇 3 個字母設置齒輪，再發送隨機選擇的 3 個字母幫助密文接受方將 Enigma 配置成相同設置來解碼。其中有個一個名為 **Wal**ter 的電報員，每天都將他的 Enigma 齒輪設置成他名字的前三個字母 W A L，然後發送的 3 個字母是他女朋友名字 **Kal**are 的前三個字母 K A L
  - 人很難真正做到隨機，所以大家用了很多讓人能猜的 Enigma 設置，比如 LON 後面跟 DON，BER 後面跟 LIN，HIT 後面跟 LER 等

- Turing 主要參與的是破譯德國海軍的 Enigma 工作，海軍 Enigma 管理更嚴格，海軍不允許電報人員像空軍那樣自己任意選擇 6 個字母 (3 個設置齒輪, 3 個發送)，字母必須從一本用水溶墨水印刷的密碼本上選取，所以破譯難度更大

- Turing 主要參與的是破譯德國海軍的 Enigma 工作，海軍 Enigma 管理更嚴格，海軍不允許電報人員像空軍那樣自己任意選擇 6 個字母 (3 個設置齒輪, 3 個發送)，字母必須從一本用水溶墨水印刷的密碼本上選取，所以破譯難度更大

- 破譯海軍 Enigma 的重要事件是 1941 年 5 月 9 日英國皇家海軍 HMS Bulldog 俘虜 u110 潛艇繳獲 Enigma Machine 和密碼本 (德軍人員急著棄船，沒有來得及銷毀密碼本)，以及 1942 年俘虜 u559 潛艇的 Enigma Machine 和密碼本。相關事件美國拍過一部電影，就是《獵殺 U-571》

- Turing 主要參與的是破譯德國海軍的 Enigma 工作，海軍 Enigma 管理更嚴格，海軍不允許電報人員像空軍那樣自己任意選擇 6 個字母 (3 個設置齒輪, 3 個發送)，字母必須從一本用水溶墨水印刷的密碼本上選取，所以破譯難度更大

- 破譯海軍 Enigma 的重要事件是 1941 年 5 月 9 日英國皇家海軍 HMS Bulldog 俘虜 u110 潛艇繳獲 Enigma Machine 和密碼本 (德軍人員急著棄船，沒有來得及銷毀密碼本)，以及 1942 年俘虜 u559 潛艇的 Enigma Machine 和密碼本。相關事件美國拍過一部電影，就是《獵殺 U-571》

- Heil Hitler 是一個 **crib**，在 Bletchley Park，他們用某些德語中的已知固定搭配或者已知信息作為解碼的 key，這些 key 叫 crib，因為 Enigma 被設計成對於任意相同的電文所輸出的密文不含有重複字元，所以可以用 crib 比對找出 crib 在電文中的可能位置來幫助破解當日的 Enigma 設置

- Turing 主要參與的是破譯德國海軍的 Enigma 工作，海軍 Enigma 管理更嚴格，海軍不允許電報人員像空軍那樣自己任意選擇 6 個字母 (3 個設置齒輪, 3 個發送)，字母必須從一本用水溶墨水印刷的密碼本上選取，所以破譯難度更大

- 破譯海軍 Enigma 的重要事件是 1941 年 5 月 9 日英國皇家海軍 HMS Bulldog 俘虜 u110 潛艇繳獲 Enigma Machine 和密碼本 (德軍人員急著棄船，沒有來得及銷毀密碼本)，以及 1942 年俘虜 u559 潛艇的 Enigma Machine 和密碼本。相關事件美國拍過一部電影，就是《獵殺 U-571》

Known plaintext attack

- Heil Hitler 是一個 **crib**，在 Bletchley Park，他們用某些德語中的已知固定搭配或者已知信息作為解碼的 key，這些 key 叫 crib，因為 Enigma 被設計成對於任意相同的電文所輸出的密文不含有重複字元，所以可以用 crib 比對找出 crib 在電文中的可能位置來幫助破解當日的 Enigma 設置

- Bletchley Park 後來甚至發展出了一套新戰術來人為創造 crib，Bletchley Park 要求英國皇家空軍在固定海域投放水雷，然後德國海軍巡邏人員就會用密碼彙報水雷位置，從而人為製造一個 crib，這一戰術 Bletchley Park 稱之為 **Gardening**

- Bletchley Park 後來甚至發展出了一套新戰術來人為創造 crib，Bletchley Park 要求英國皇家空軍在固定海域投放水雷，然後德國海軍巡邏人員就會用密碼彙報水雷位置，從而人為製造一個 crib，這一戰術 Bletchley Park 稱之為 **Gardening**
- 但即使這樣，比對 **cribs** 仍是一個耗時的工作，Turing 的主要貢獻是把這個機械性耗費人力的工作用機器取代，他提出的自動邏輯計算模型，幫助工程師製造出了一個自動搜索機器 Bombe

- Bletchley Park 後來甚至發展出了一套新戰術來人為創造 crib，Bletchley Park 要求英國皇家空軍在固定海域投放水雷，然後德國海軍巡邏人員就會用密碼彙報水雷位置，從而人為製造一個 crib，這一戰術 Bletchley Park 稱之為 **Gardening**
- 但即使這樣，**比對 cribs** 仍是一個耗時的工作，Turing 的主要貢獻是把這個機械性耗費人力的工作用機器取代，他提出的自動邏輯計算模型，幫助工程師製造出了一個自動搜索機器 Bombe
- 用 **crossword puzzle** 招募人員是 Bletchley Park 一直在做的工作，不是 Turing 想出來的。招募的人員的背景龐雜，從語言學家到古埃及學家，甚至還有律師

- Bletchley Park 後來甚至發展出了一套新戰術來人為創造 crib，Bletchley Park 要求英國皇家空軍在固定海域投放水雷，然後德國海軍巡邏人員就會用密碼彙報水雷位置，從而人為製造一個 crib，這一戰術 Bletchley Park 稱之為 **Gardening**
- 但即使這樣，**比對 cribs** 仍是一個耗時的工作，Turing 的主要貢獻是把這個機械性耗費人力的工作用機器取代，他提出的自動邏輯計算模型，幫助工程師製造出了一個自動搜索機器 Bombe
- 用 **crossword puzzle** 招募人員是 Bletchley Park 一直在做的工作，不是 Turing 想出來的。招募的人員的背景龐雜，從語言學家到古埃及學家，甚至還有律師
- 我們用的電腦不是 **Turing Machine**，Turing Machine 是一個理論上的計算模型，是有限狀態機的延伸：
  http://en.wikipedia.org/wiki/Turing_machine