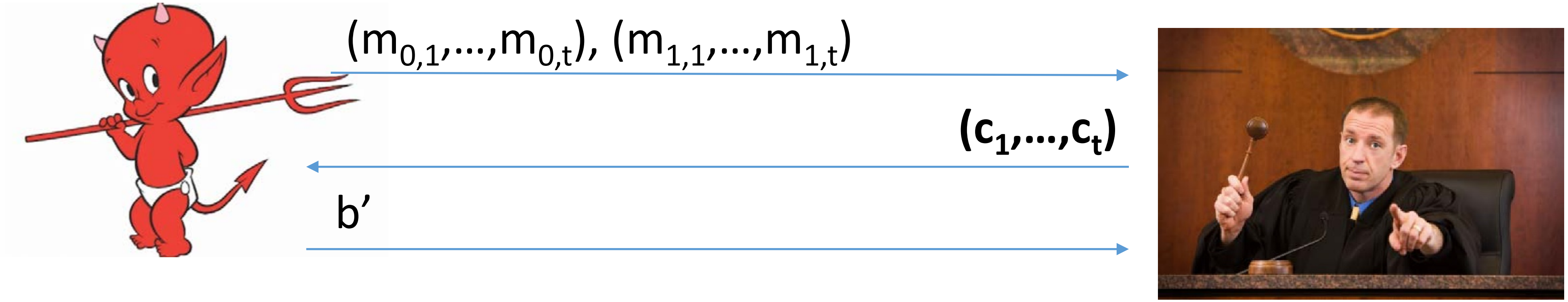
Cryptography
CS 555

Topic 6: Constructing Secure Encryption Schemes

Recap

- Sematic Security/Indistinguishable Encryptions against eavesdropping attacker with one ciphertext
- Pseudorandom Number Generators

Multiple Message Eavesdropping Experiment



Random bit b

K = Gen(.)

c_i = $Enc_K(m_{b,i})$

ppt attacker

negligible function

$\forall$ $\Pr\Big[$ $Guesses\ b' = b\Big] \le \frac{1}{2} + \mu(n)$

Multiple Message Eavesdropping Experimen

om bit b

en(.)

$c_K(m_b)$

$Formally, let\ \Pi = (Gen, Enc, Dec)\ denote\ the\ encryption\ scheme,$
$call\ the\ experiment\ PrivK^{mult}\ and\ define\ a\ random\ variable$

$$PrivK_{A,\Pi}^{mult} = 1 \quad if\ b = b'$$
$$PrivK_{A,\Pi}^{mult} = 0 \quad otherwise$$

$\Pi\ has\ indistinguishable\ multiple\ encryptions\ in\ the\ presence\ of$
$an\ eavesdropper\ if\ for\ all\ PPT\ adversary\ A, there\ is\ a$
Negligible function μ such that $\Pr[PrivK_{A,\Pi}^{mult} = 1] \leq \frac{1}{2} + \mu(n)$

$[$

$] = 2 \quad ( )$

A Simple Observation

If Π has ***indistinguishable multiple encryptions*** in the presence of an eavesdropper

then

Π also has **indistinguishable encryptions** in the presence of an eavesdropper.

- In fact ***indistinguishable multiple encryptions*** *is a strictly stronger security notion.*

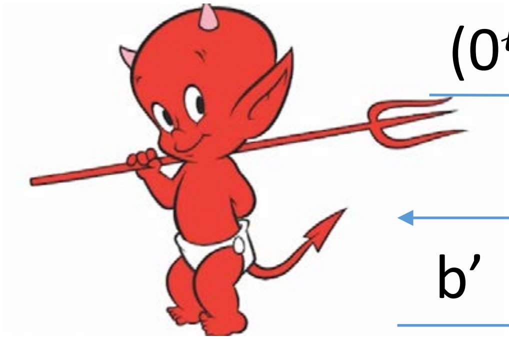
Example

$$\mathrm{Enc}_{\mathrm{s}}(\mathrm{m}) = \mathrm{G}(\mathrm{s}) \oplus m$$
$$\mathrm{Dec}_{\mathrm{s}}(\mathrm{c}) = \mathrm{G}(\mathrm{s}) \oplus c$$

Recall: $\Pi = (Gen, Enc, Dec)$ has **indistinguishable encryptions** in the presence of an eavesdropper.

Claim: $\Pi = (Gen, Enc, Dec)$ does **not** have **indistinguishable multiple encryptions** in the presence of an eavesdropper.

Multiple Message Eavesdropping



$(0^{\ell(n)}, 0^{\ell(n)}), (0^{\ell(n)}, 1^{\ell(n)})$

$(G(s)\oplus \mathbf{m}_{b,1}, G(s)\oplus \mathbf{m}_{b,2})$

b’

Random bit b

s = Gen(.)

$c_i = Enc_K(m_{b,i})$

$$b' = \begin{cases} 1 & \text{if } c_1 = c_2 \\ 0 & \text{otherwise} \end{cases}$$

Analysis: If b=1 then $c_1 = G(s)\oplus 0^{\ell(n)} = c_2$

Analysis: If b=0 then $c_1 = G(s)\oplus 0^{\ell(n)} \neq G(s)\oplus 1^{\ell(n)} = c_2$

Did We Cheat?

- Attack specifically exploited the fact that we can ask to see multiple encryptions of the same message…
- The above argument might appear to show that no encryption scheme provides secure **indistinguishable multiple encryptions** in the presence of an eavesdropper.

Theorem: If Π is (stateless) encryption scheme and Enc is deterministic then Π does **not provide** secure **indistinguishable multiple encryptions**

Did We Cheat?

Option 1: Weaken the security definition so that attacker cannot request two encryptions of the same message.

- Undesirable!
- **Example:** Dataset in which many people have the last name “Smith”
- We will actually want to strengthen the definition later…

Option 2: Consider randomized encryption algorithms

Chosen-Plaintext Attacks

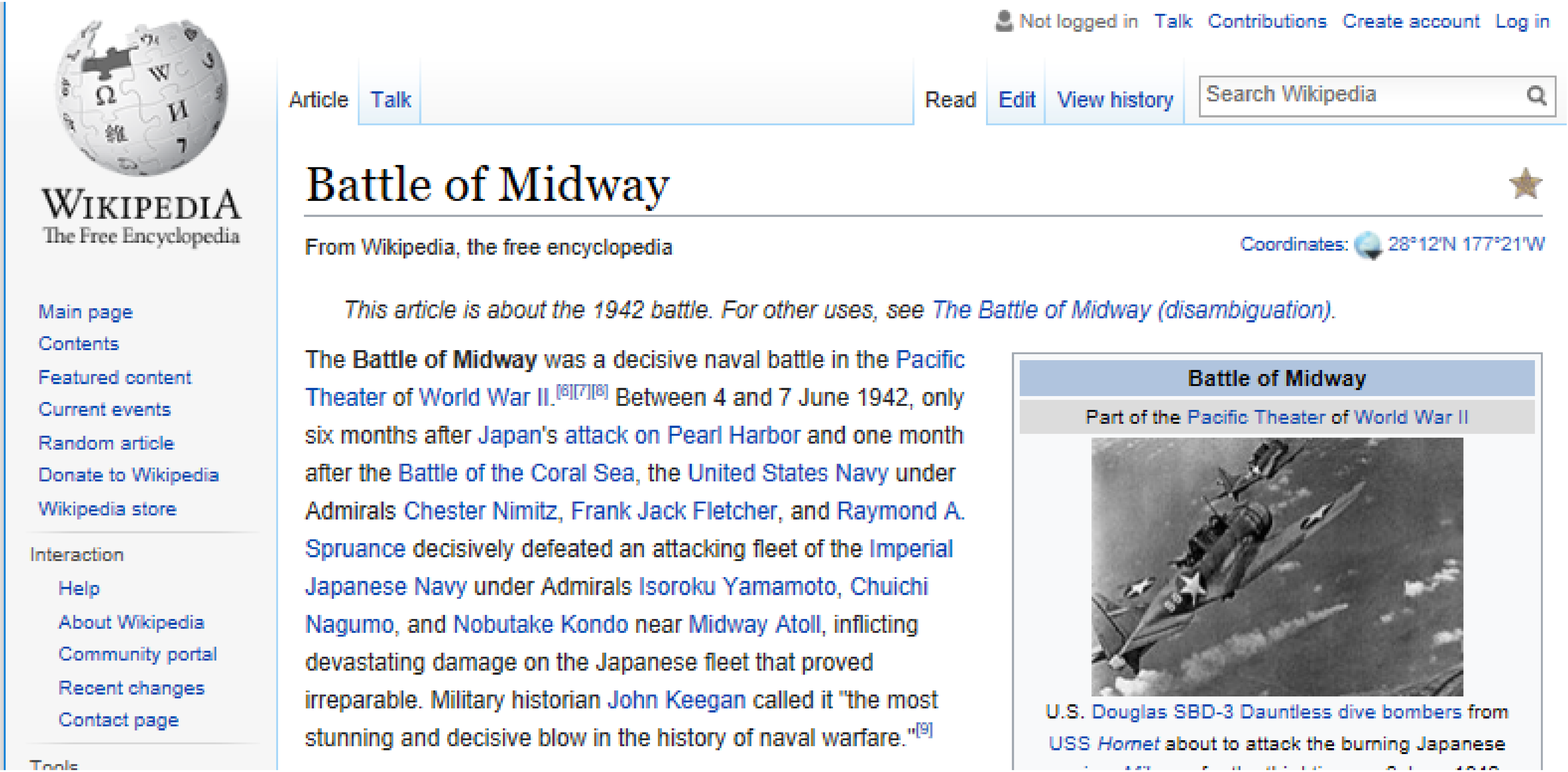
- Model ability of adversary to control or influence what the honest parties encrypt.

- During World War 2 the British placed mines at specific locations, knowing that the Germans, upon finding the mines, would encrypt the location and send them back to headquarters. The encrypted messages helped cryptanalysts at Bletchley Park to break the German encryption scheme.

Chosen-Plaintext Attacks

- Model ability of adversary to control or influence what the honest parties encrypt.

- Battle of Midway (WWII). US Navy cryptanalysts intercept and encrypted message which they are able to partially decode (May 1942).
  - The message stated that the Japanese were planning an attack on AF?
  - Cryptanalysts could not decode ciphertext fragment AF.
  - Best Guess: AF = “Midway Island.”



Battle of Midway

From Wikipedia, the free encyclopedia

Coordinates: 28°12′N 177°21′W

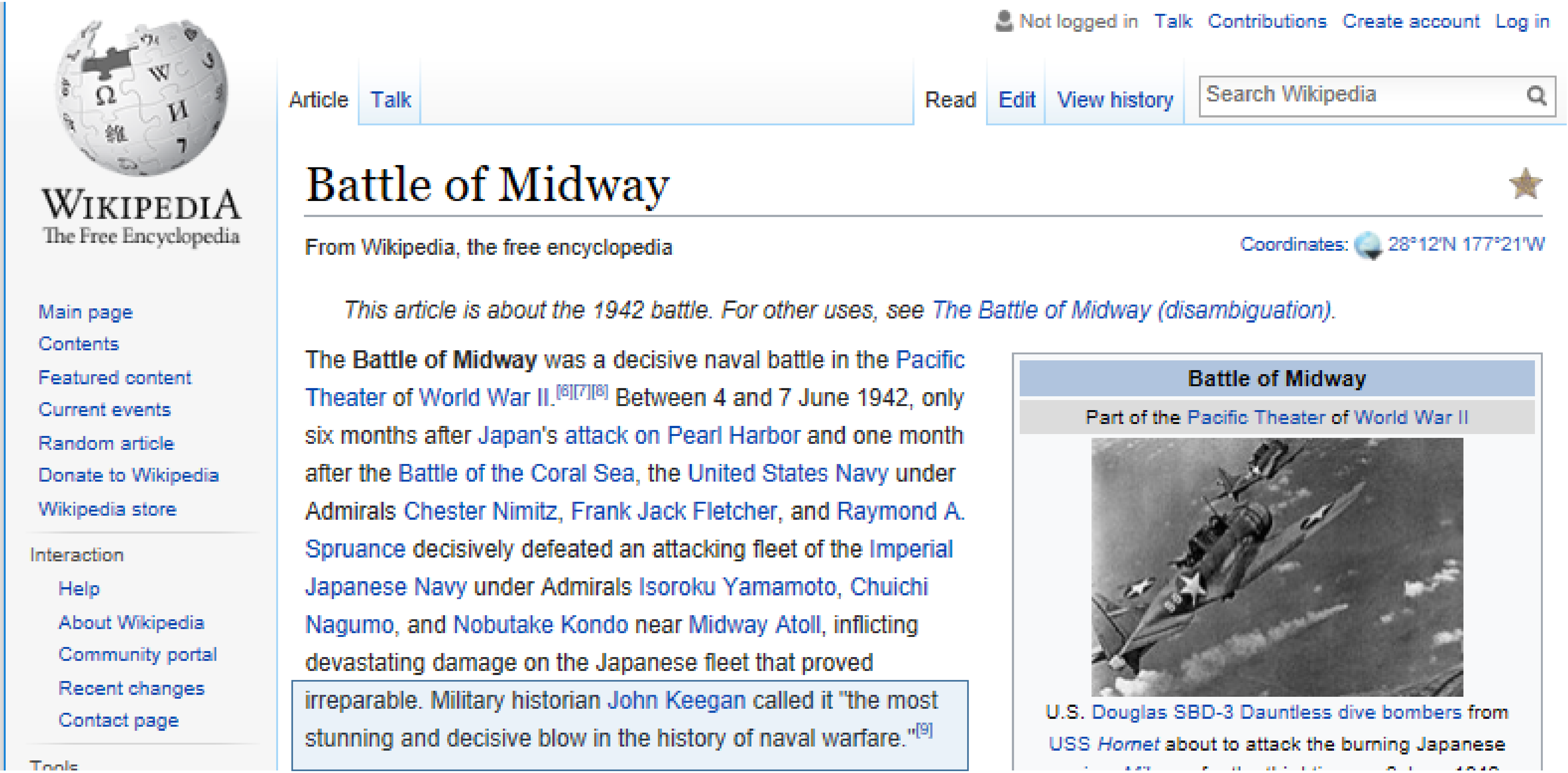
This article is about the 1942 battle. For other uses, see The Battle of Midway (disambiguation).

The **Battle of Midway** was a decisive naval battle in the Pacific Theater of World War II.[6][7][8] Between 4 and 7 June 1942, only six months after Japan's attack on Pearl Harbor and one month after the Battle of the Coral Sea, the United States Navy under Admirals Chester Nimitz, Frank Jack Fletcher, and Raymond A. Spruance decisively defeated an attacking fleet of the Imperial Japanese Navy under Admirals Isoroku Yamamoto, Chuichi Nagumo, and Nobutake Kondo near Midway Atoll, inflicting devastating damage on the Japanese fleet that proved irreparable. Military historian John Keegan called it "the most stunning and decisive blow in the history of naval warfare."[9]

Battle of Midway

Part of the Pacific Theater of World War II

U.S. Douglas SBD-3 Dauntless dive bombers from USS *Hornet* about to attack the burning Japanese



Battle of Midway

From Wikipedia, the free encyclopedia

Coordinates: 28°12′N 177°21′W

This article is about the 1942 battle. For other uses, see The Battle of Midway (disambiguation).

The **Battle of Midway** was a decisive naval battle in the Pacific Theater of World War II.[6][7][8] Between 4 and 7 June 1942, only six months after Japan's attack on Pearl Harbor and one month after the Battle of the Coral Sea, the United States Navy under Admirals Chester Nimitz, Frank Jack Fletcher, and Raymond A. Spruance decisively defeated an attacking fleet of the Imperial Japanese Navy under Admirals Isoroku Yamamoto, Chuichi Nagumo, and Nobutake Kondo near Midway Atoll, inflicting devastating damage on the Japanese fleet that proved irreparable. Military historian John Keegan called it "the most stunning and decisive blow in the history of naval warfare."[9]

Battle of Midway

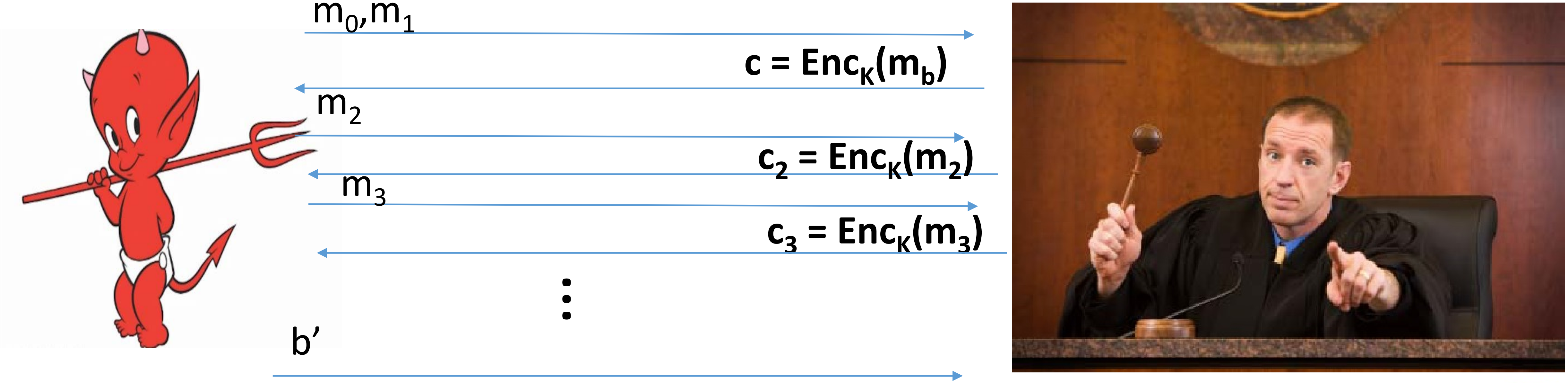
Part of the Pacific Theater of World War II

U.S. Douglas SBD-3 Dauntless dive bombers from USS *Hornet* about to attack the burning Japanese

Multiple Message Security and CPA-Attacks

- Multiple Message Security
  - Attacker must select all messages at the same time.
  - Significant Limitation!
- In the WWII attacks cryptanalysts selected the message adaptively
  - Selected message(s) to encrypt *after* observing target ciphertext

CPA-Security (Single Message)



m_0,m_1

$\mathbf{c = Enc_K(m_b)}$

m_2

$\mathbf{c_2 = Enc_K(m_2)}$

m_3

$\mathbf{c_3 = Enc_K(m_3)}$

⋮

b'

Random bit b

K = Gen(.)

$$\forall PPT\ A\ \exists \mu\ (\text{negligible})\ \text{s.t}$$

$$\Pr[A\ \ Guesses\ b' = b] \leq \frac{1}{2} + \mu(n)$$

CPA-Security (Single Message)

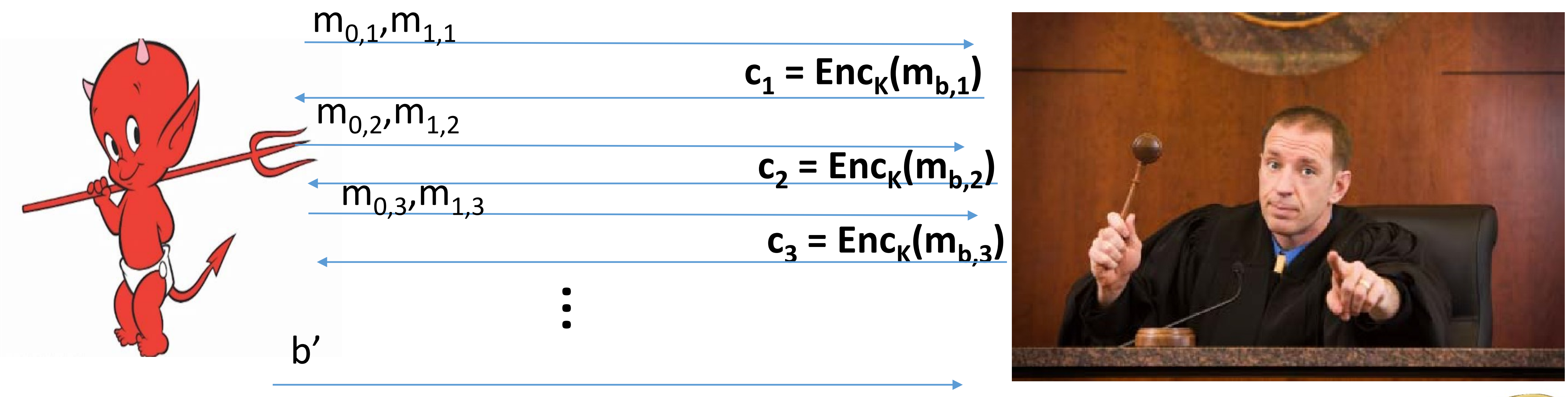
Formally, let $\Pi = (Gen, Enc, Dec)$ *denote the encryption scheme, call the experiment* $PrivK^{cpa}$ *and define a random variable*

$$PrivK_{A,\Pi}^{cpa} = 1 \quad if\ b = b'$$
$$PrivK_{A,\Pi}^{cpa} = 0 \quad otherwise$$

Π *has indistinguishable encryptions under a chosen plaintext attack if for all PPT adversaries* A, *there is a* negligible function μ such that

$$\Pr[PrivK_{A,\Pi}^{cpa} = 1] \leq \frac{1}{2} + \mu(n)$$

CPA-Security (Multiple Messages)



$m_{0,1}, m_{1,1}$

$c_1 = \mathrm{Enc}_K(m_{b,1})$

$m_{0,2}, m_{1,2}$

$c_2 = \mathrm{Enc}_K(m_{b,2})$

$m_{0,3}, m_{1,3}$

$c_3 = \mathrm{Enc}_K(m_{b,3})$

⋮

b’

Random bit b

K = Gen(.)

$$\forall PPT\ A\ \exists \mu\ \text{(negligible) s.t}$$

$$\Pr[A\ \ Guesses\ b' = b] \leq \frac{1}{2} + \mu(n)$$

CPA-Security

Theorem: An encryption scheme $\Pi = (Gen, Enc, Dec)$ that is CPA-Secure for single encryptions is also CPA-secure for multiple encryptions.

- We will simply say CPA-security for simplicity
- To show CPA-Security it suffices to show CPA-security for single encryptions.
- To reason about security of a protocol using Π we can use game with multiple encryptions.

CPA-Security

- CPA-security vs Multiple Message Encryption
  - CPA-security is stronger guarantee
  - Attacker can select messages adaptively
- CPA-security minimal security notion for a modern cryptosystem

- Limitations of CPA-Security: Does not model and adversary who
  - Attempts to modify messages
  - Can get honest party to (partially) decrypt some messages

CPA-Security and Message Length

Observation: Given a CPA-secure encryption scheme $\Pi = (Gen, Enc, Dec)$ that supports messages of a single bit ($\mathcal{M} = \{0,1\}$) it is easy to build a CPA-secure scheme Π'$= (Gen', Enc', Dec')$ that supports messages m = m_1,…,m_n∈ $\{0,1\}^n$ of length n.

$$\mathrm{Enc}_{\mathrm{k}}'(m) = \mathrm{Enc}_{\mathrm{k}}'(m_1), \ldots, \mathrm{Enc}_{\mathrm{k}}'(m_n)$$

Exercise: How would you prove Π' is CPA-secure?

Next Class

- Read Katz and Lindell 3.5-3.6.1
- Constructing CPA-Security with Pseudorandom Functions