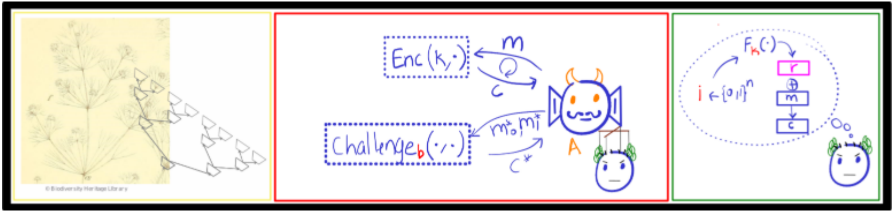


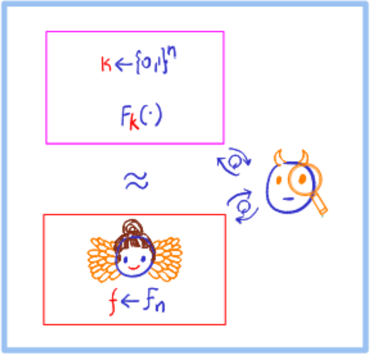
CS409m: Introduction to Cryptography

Lecture 08 (29/Aug/25)

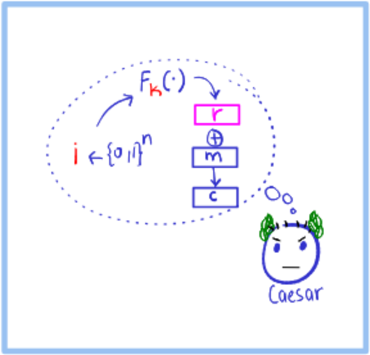
Instructor: Chethan Kamath

- Task: secure communication of *multiple messages* with shared keys
- Threat model: computational secrecy against eavesdroppers (EAV*)

Pseudo-Random Function (PRF)

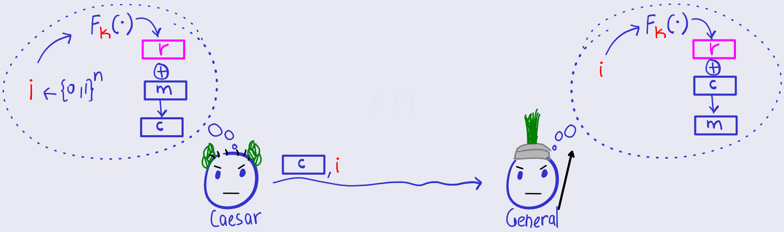


PRF $\Longrightarrow$ EAV*-secure SKE



Recall from Previous Lecture...

Construction 1 (Lecture 07, PRF $\implies$ SKE)



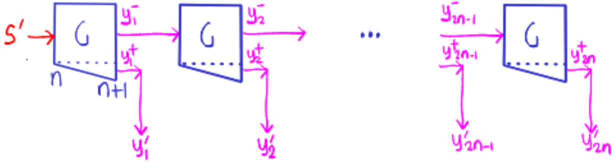
Theorem 1

If F *is a PRF, then Construction 1 (Lecture 07) is EAV*-secure*

Proof.

Similar to proof of PRG $\implies$ EAV-SKE □

But How to Construct a PRF?



- Recall construction of length-extending PRG from Lecture 06-07
- Recall the problem with expanding exponentially:
  - Takes exponential time to access most pseudorandom OTPs

Need "PRG" with

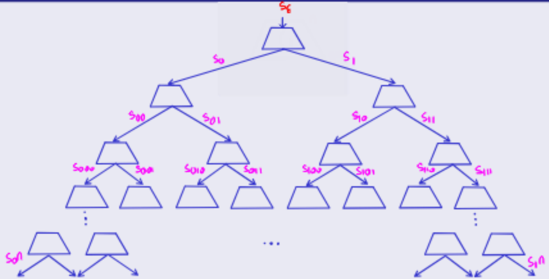
1. Exponential stretch
2. Output bits "efficiently" accessible (also called locality)

How to reconcile the two requirements?

- Hint: Use length-doubling PRG
- Use binary tree instead of chain!

Tree-Based Construction from Length-Doubling PRG G

Construction 2 (GGM PRF $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$)

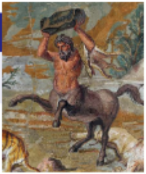


Define $F_k(x) = s_x$ with $s_\varepsilon := k$

Theorem 2

If G is a length-doubling PRG, then Construction 2 is a PRF.

Proof: a "frugal" hybrid argument: see [Gol01, §3.6].

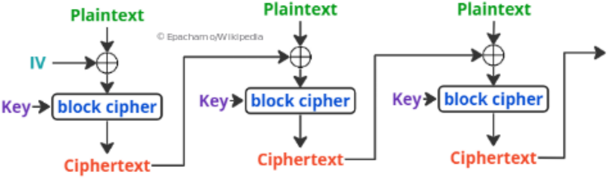


©Wikipedia

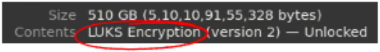
PRFs IRL

- Practical PRFs: block ciphers like AES
  - − Usually only support certain key-sizes (128, 192, 256)
  - + Supported by most libraries (e.g., OpenSSL, NaCl) and even implemented on modern processors (AES-NI)

- Coming up in Lecture 09: for encrypting long messages (e.g., for disk encryption) "modes of operation" used
  - E.g: Cipher block-chaining (CBC) mode



  - My laptop uses LUKS for disk encryption, which uses AES-XTS

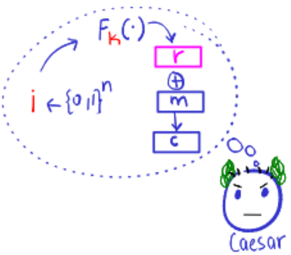


Plan for Today's Lecture

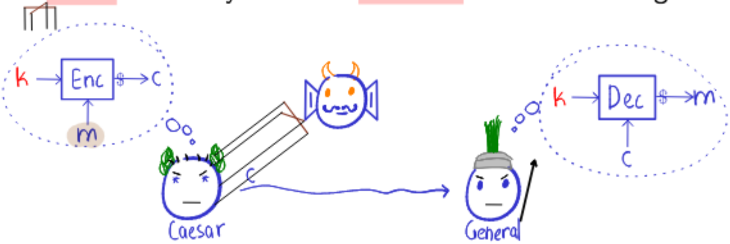
- Task: secure comm. of multiple messages with shared keys
- Threat model: comp. secrecy against chosen-plaintext attack (CPA)

Chosen-Plaintext Attack (CPA)

PRF $\Longrightarrow$ CPA-secure SKE



- Recall computational secrecy against eavesdroppers (EAV/EAV*)
- CPA: *active* adversary who can influence Caesar's messages

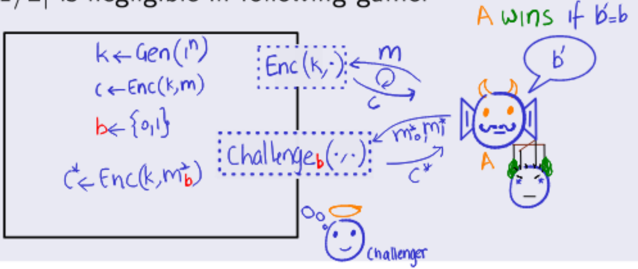


Chosen-Plaintext Attack (CPA)

- Recall computational secrecy against eavesdroppers (EAV/EAV*)
- CPA: *active* adversary who can influence Caesar's messages

Definition 1 (Indistinguishability against CPA)

An SKE $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CPA-secure if for *every* PPT attacker A $|\Pr[b' = b] - 1/2|$ is negligible in following game.



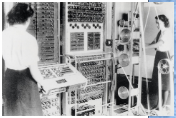
Exercise 1

Prove that if an SKE Π is CPA-secure then it is EAV-secure.

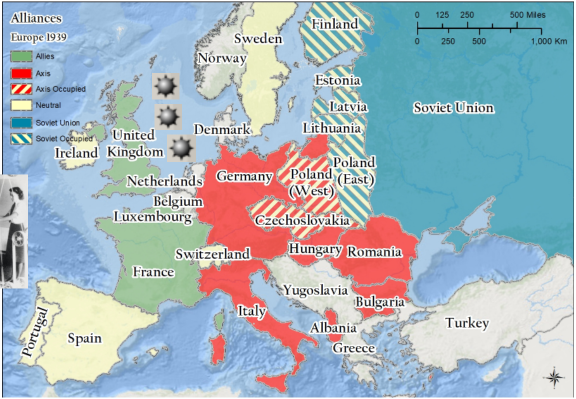
Chosen-Plaintext Attack IRL

- "[...] during World War II, British placed mines at certain locations, knowing that the Germans—when finding those mines—would encrypt the locations and send them back to headquarters." [KL14]

© Rocky Acosta/Wikipedia



© Wikipedia



© Steve Banas/cod.pressbooks.pub

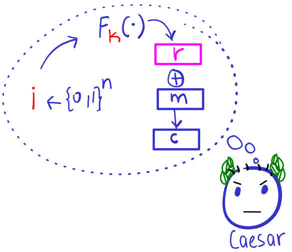
- Computer viruses might not have access to secret key, but can still send encrypted messages

Plan for Today's Lecture

- Task: secure comm. of *multiple messages* with shared keys
- Threat model: comp. secrecy against chosen-plaintext attack (CPA)

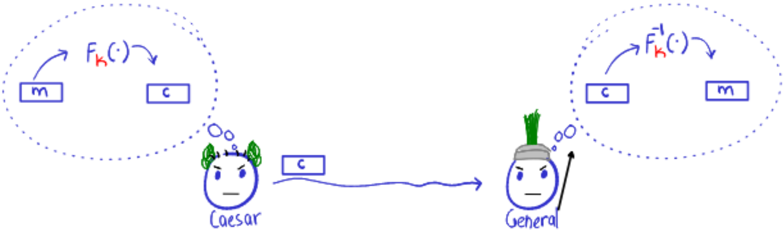
NEW Chosen-Plaintext Attack (CPA)

PRF $\Longrightarrow$ CPA-secure SKE NEW



How to Construct CPA-Secure SKE?

- Attempt 1: consider the PRF-based scheme $\mathrm{Enc}(k, m) := \mathrm{F}_k(m)$
  - Assume $\forall k \in \{0,1\}^n$, $F_k : \{0,1\}^n \to \{0,1\}^n$ is a *permutation* (more on this in Lecture 09!)



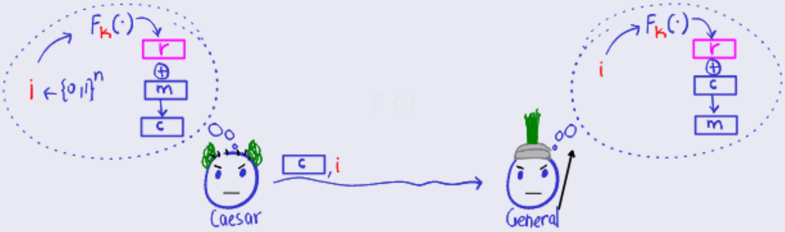
Do you think it is CPA-secure? No! How to attack? E.g.:

1. Query encryption oracle on $0^n \in \{0,1\}^n$ to obtain c
2. Challenge on $(0^n, 1^n)$ to obtain c^*
3. Output $b' = 0$ if $c = c^*$

Takeaway: CPA-secure SKE *cannot* have deterministic Enc!

What About PRF-based SKE from Lecture 07?

Construction 1 (Lecture 07, PRF $\Longrightarrow$ SKE)



- Is Enc deterministic? No, so the trivial attack won't work
- Do you think it is CPA-secure?

Theorem 3

If F *is a PRF, then Construction 1 (Lecture 07) is CPA-secure.*

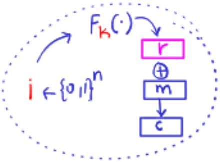
- Proof on whiteboard

Recap/Next Lecture

- Defined an "active" threat model: CPA
  - CPA adversary can control the messages to be encrypted

  ⚠ Enc deterministic $\implies$ CPA-insecure!

- Constructed a (stateless) CPA-secure SKE from PRF



- Next lecture
  - Block cipher a/k/a pseudo-random permutation (PRP)
  - *Modes of operation* for efficiently encrypting *long* messages

Further Reading

1. [Gol01, §3.6] for a formal proof of Theorem 2
2. You can find a formal treatment of PRF-based SKE in [KL14, §3.5.2] – in particular, Theorem 1 is Theorem 3.29 there, and a formal proof follows.

Oded Goldreich.
The Foundations of Cryptography - Volume 1: Basic Techniques.
Cambridge University Press, 2001.

Jonathan Katz and Yehuda Lindell.
Introduction to Modern Cryptography (3rd ed.).
Chapman and Hall/CRC, 2014.