# How to Use Your Block Cipher?

Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
India
palash@isical.ac.in

IACITS
New Delhi, 2nd April 2009



# Block Cipher

$$E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$$

- **key space**: $\mathcal{K} = \{0,1\}^k$.
- **message and cipher spaces**: $\mathcal{M} = \{0,1\}^n, \mathcal{C} = \{0,1\}^n$.
- $E_K(M) = E(K, M)$ is a permutation for every fixed $K$.
- Typical values:
  $n, k = 128, 192, 256$.



# Choose Your Block Cipher

- **Public domain approach**: AES, DES, IDEA, MARS, SERPENT, RC6, ...
  - AES: standardised by the NIST (USA) for encryption of “sensitive (unclassified)” information; FIPS 197, November 26, 2001.
- **Proprietary approach**:
  **pros**: benefit from “security by obscurity”;
  **cons**: cannot benefit from third party cryptanalysis.
- **Mixed approach**:
  - start from a public domain block cipher;
  - introduce additional structure and generalize to a large family of block ciphers;
  - pick a random block cipher from the family.



# How Secure Is Your Block Cipher?

- **Resists "known" attacks**.
  - Linear and Differential Attacks.
  - Slide, Rectangle, Impossible Differential, Boomerang and other attacks.
- **Pseudo-random permutation (PRP)**: indistinguishable from a random permutation where the adversary is allowed to ask for encryptions.
- **Strong pseudo-random permutation (SPRP)**: indistinguishable from a random permutation where the adversary is allowed to ask for encryptions *and decryptions*.



# Your Block Cipher is Secure

**Assumption:** the block cipher is “perfectly secure” (whatever that may mean).

**Is that the end of the story?**

**No!**



# Your Block Cipher and Your Requirement

**Block length.**

- The block cipher handles $n$-bit blocks.
- Typically, $n = 128, 192$ or $256$ bits.

**Message Requirements.**

- Handle “long” messages.
- Handle “variable” length messages.
- Handle fixed length messages (a disk sector).



# Your Block Cipher and Your Requirement

**Secure Block Cipher.**

- The block cipher ensures strong security for $n$-bit blocks.

**Different Security Requirements.**

- Privacy only.
- Authentication.
- Authenticated encryption.
- Authenticated encryption with associated data.
- Wide-block encryption.
- Disk sector encryption.
- Deterministic authenticated encryption (key wrap problem).
- On-line encryption.
- Other niche requirements.



# Modes of Operations

**Commonly known modes.**

- Electronic codebook mode (ECB).
- Counter mode (Ctr).
- Cipher block chaining mode (CBC).
- Output feedback mode (OFB).
- Cipher feedback mode (CFB).



# Things to Note

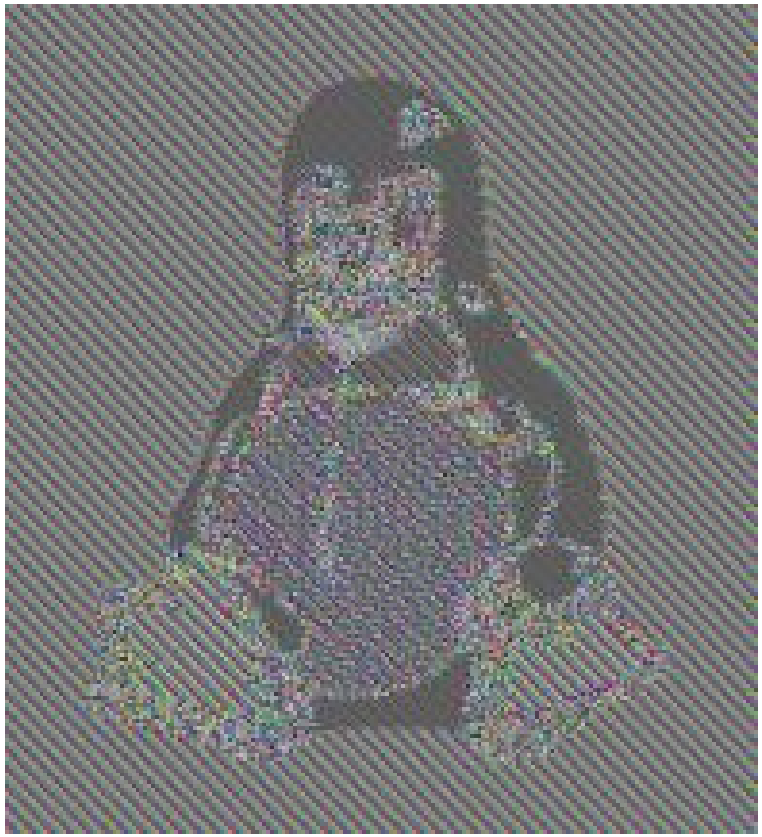
- ECB does not provide privacy.
- Ctr provides privacy but not authentication.
- CBC provides authentication, but, not authenticated encryption.
- Authenticated encryption with associated data?
- Wide block encryption?
- Disk encryption?
- Other security requirements?

**There is no single mode which can be used for all applications.**



# Insecurity of ECB Mode





**Source: Wikipedia**

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

# Authentication

**Goal:** detect tampering of the message.
**Solution:** sender generates tags; receiver verifies them;
sender and receiver share a common key.

- **Sequential.** CMAC (NIST-standard).
  based on CBC;
  design by Iwata-Kurosawa and based on earlier work by others.
- **Parallel.**
  - PMAC: Black-Rogaway; Rogaway.
  - Generalization of PMAC to an efficient family: Chakraborty-Sarkar.
  - iPMAC: Sarkar;
    more flexible and slightly faster than PMAC.



# Authenticated Encryption

**Goal:** achieve both privacy and authentication of the message.

- **Two-pass solutions:** relatively inefficient but patent-free;
  - GCM (Viega-McGrew) – NIST standard.
- **Single-pass solutions:**
  - IACBC, IAPM (Jutla);
  - XCBC, XECB (Gligor-Donescu);
  - OCB (Rogaway);
  - Generalization of OCB to an efficient family: (Chakraborty-Sarkar);
  - Flexibility and speed-up over OCB – work under progress.



# Authenticated Encryption with Associated Data

**Associated data (header).**

- Needs to be authenticated but not encrypted.
- Example: IP packets.

**Constructions.**

- Variants of AE protocols such as OCB and its generalizations.
- Generic construction: combine any AE protocol and a collision-resistant hash function (Sarkar).



# Wide Block Encryption – Disk Encryption

**Goals.**

- Perform “strong” encryption;
- support a tweak;
- for disk encryption, the tweak is the sector address.

**Some constructions.**

- CBC, EME (Halevi-Rogaway): **2**[BC] per block;
- XCB (McGrew-Fluhrer): **1**[BC]+**2**[M] per block;
- HCtr (Wang-Feng-Wu), HCH (Chakraborty-Sarkar):
  **1**[BC]+**2**[M] per block;
  better key agility compared to XCB.
- HEH, iHCH (Sarkar): **1**[BC]+**1**[M] per block;
- further work under progress.



# Summary

- Choice of block ciphers:

  **“to be or not to be (proprietary)”.**

- But choosing a block cipher is not enough.
  - Understand the security goal.
  - Choose the appropriate mode of operation.
  - Implementation issues. (Not discussed.)
- Standards.
  - Agencies. NIST (USA), IEEE, IETF;
  - India?



# Moral of the Story

**A block cipher is like a Swiss army knife.**
**But, you have to use it properly!**



# Post-Script

**Exploding Common Myths.**

- Cryptography means you have to garble up bits and bytes. Any electronics engineer can do it. **Wrong!**
- Good mathematician $\Rightarrow$ Good cryptologist. **Wrong!**

**Sensible Facts About Cryptology.**

- Interdisciplinary: mathematics, computer science, engineering.
- Requires specialised knowledge.
- Serious and challenging (academic) discipline.



**Thank you for your attention!**

