Block Ciphers

Based on *Cryptography Engineering* sections 3.3, 3.4 By Ferguson, Schnier, and Kohno

Lecture notes of Alexander Wood
awood@jjay.cuny.edu

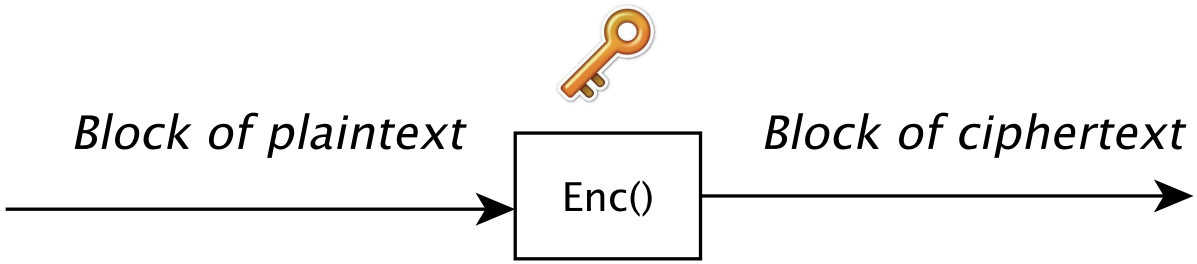
John Jay College of Criminal Justice

What is a block?

A **block** is a chuck of data of a predetermined size. For instance a block of 64 contiguous bits.

When encrypting with blocks, we encrypt data block-by-block.

Block Encryption



Identical blocks should be encrypted to different ciphertexts! To do this we must introduce a notion of **randomness**, one of the most important concepts in cryptography.

Block Size: Not Too Small!

With a bit block of size L there are 2^L possible plaintext bit combinations. A larger block size means there are more possible plaintext bits. Thus we wish to **avoid very small blocks**.

Block Size: Not Too Large!

A block size too large makes the ciphertext too inefficient to work with. **Avoid very large blocks**.

Block Size: Just Right!

Preferred block sizes are **multiples of 8** since most processors handle data in multiples of 8 (ie, the length of a byte).

Padding a Block Cipher

When a plaintext is shorter than the desired block size it is **padded** with redundant information, making the last block the necessary block size.

Padding should be randomized each time it is applied. Too much padding can make the system inefficient. (Hence, the need to avoid too large of a block size!)

Block Cipher Schemes

- **Digital Encryption Standard (DES)** ← Next class!
- Triple DES
- Advanced Encryption Standard (AES)
- IDEA
- Twofish
- Serpent

What is block cipher security?

???

What is block cipher security?

It's difficult to formalize! We give a "sketch" of the definition in these slides.

Ideal Block Ciphers

We define block cipher security in relation to an **ideal block cipher**. An ideal block cipher is a random permutation, meaning:

- For each key, the block cipher is a **random** permutation
- The key-permutation pairs shold be chosen **randomly**

Ideal Block Ciphers

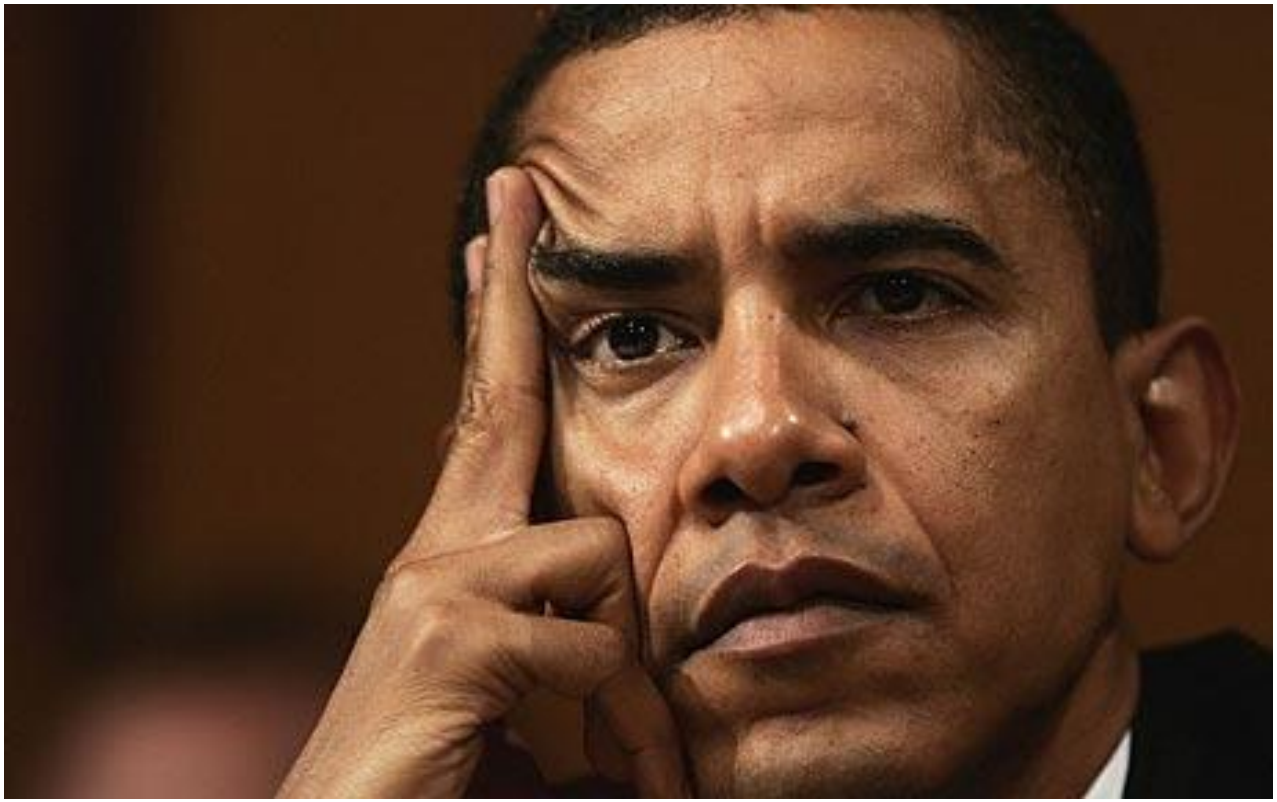
A more formal definition would introduce a **uniform probability distribution** over the set of all *possible* block ciphers.

Block Cipher Security (Informal Definition)

A block cipher is **secure** if no attack against it exists.

Block Cipher Security (Informal Definition)

Okay.. but what does this mean?



Attack Against A Block Cipher

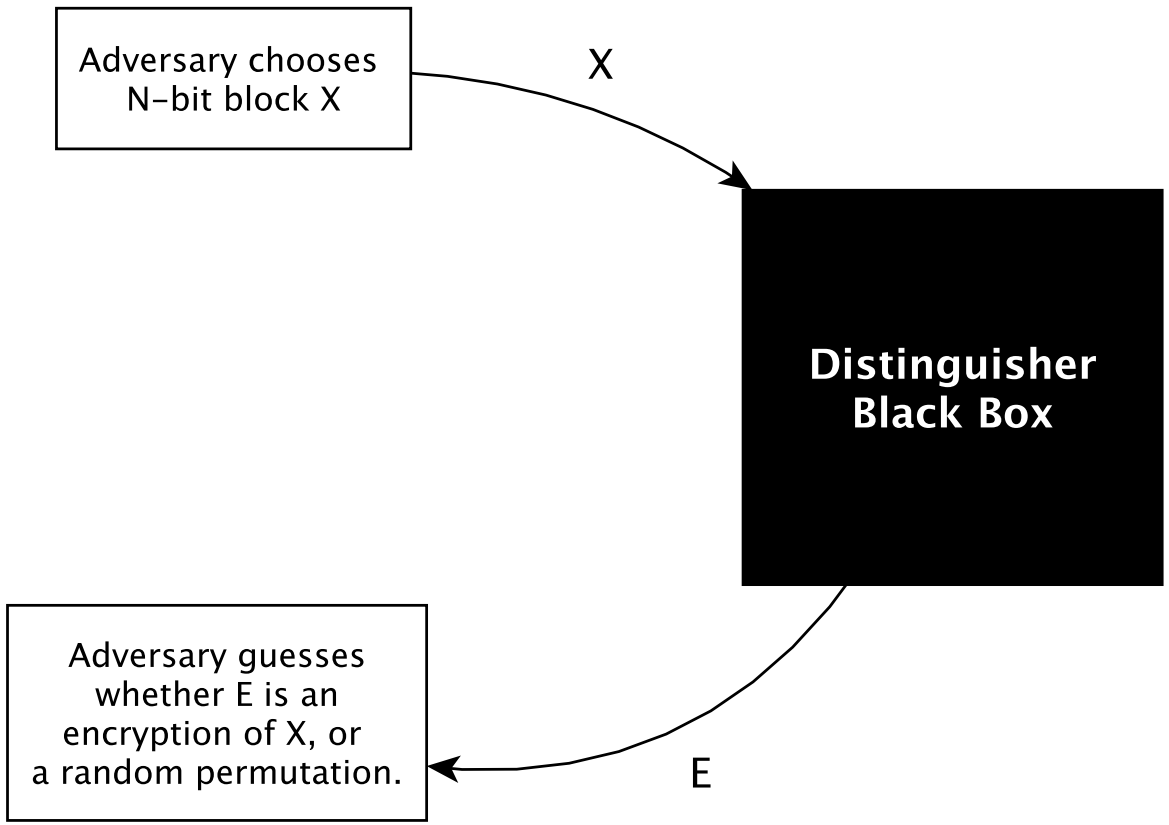
A method of distinguishing between a given block cipher and an ideal block cipher is called an **attack** on the given block cipher.

Okay.. but what does “distinguishing” mean?

Distinguishers

A **distinguisher** is a black-box function which provides means to compare a given block cipher to the “ideal” construct of a block cipher.

Distinguishers



Computational Distinguishability

There are various types of indistinguishability. In Cryptography we often look at **computational indistinguishability** – given a certain amount of computational resources, can the distinguisher function tell the difference between the given scenario and the ideal scenario?

Distinguishers

The distinguisher is a theoretical model. It has access to both the encryption, decryption, and key generation functions. It is free to choose any key during its operations.

The adversary does *not* know whether the black box is implementing the block cipher or the ideal block cipher.

The job of the adversary is to determine whether the ideal or the given block cipher is being implemented by the black box function.

Distinguishers

Note that the adversary does not have to get it right every time! It only has to get it right more often than not.

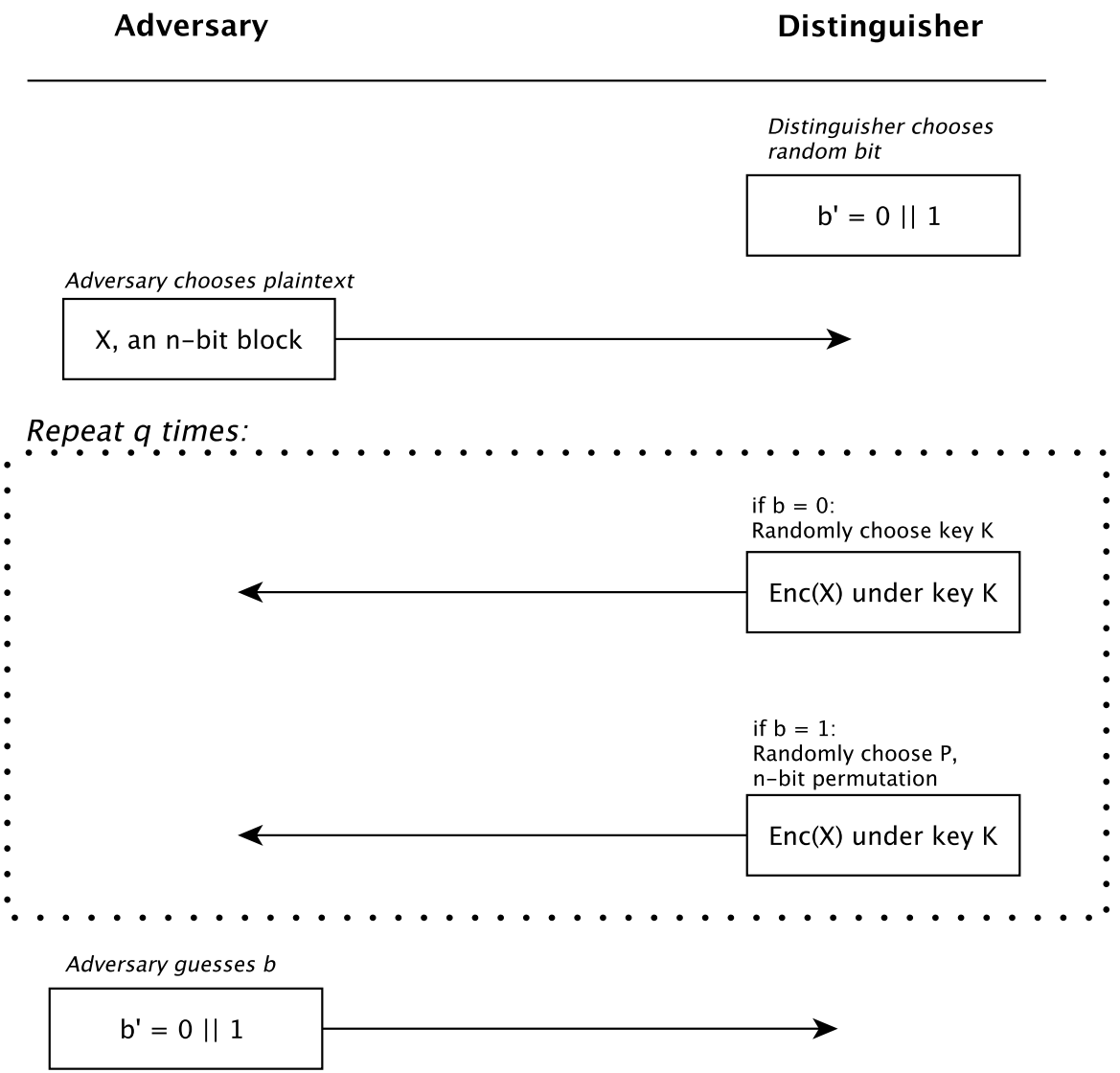
This means that with a probability more than negligibly greater than 50%, the adversary can tell you whether the black box is running with the given block cipher or with an ideal block cipher.

Distinguisher Game

Let E be an n-bit block cipher and D a distinguisher.

- D randomly chooses a bit 0 or 1.
- The attacker chooses an n-bit block X and sends it to the distinguisher.
- The distinguisher D carries out the following:
  - If D chose 0, then D chooses a random key K and will output $\texttt{Enc}_K(X)$.
  - If D chose 1, then D will output a random permutation of length n.
- Step 2 is repeated q times.
- The attack guesses the bit 0 or 1 and wins if the guess is correct.

Distinguisher Game



Example 1: A Trivial Distinguisher

Encrypt the plaintext 0 with the key 0. See if the result matches what we expect from a block cipher X.

This is called *trivial*, or *generic*. When looking at block cipher security we need to look at *non-generic* cases.

What is non-generic

The book explains: “it’s a bit like an obscenity: we know it when we see it.”

What is non-generic?

We can do a bit better than that.

The generic attack above is so simple that we could even use it to distinguish between two ideal block ciphers.

We want an attack that exploits the internal properties of the block themselves.

Example 2: More Complicated, But Generic

Encrypt the plaintext 0 with all keys in the range $1, \ldots, 2^{32}$. Count how often each value for the first 32 bits of ciphertext occurs.

If a value repeats 5 times, instead of the expected 1 time which would happen with a random block, then we have found a property which is unlikely to hold for an ideal block.

Example 2: More Complicated, But Generic

However this distinguisher is still generic! It is still applicable to *all* block ciphers and does not use the properties of the *given* block cipher X.

Example 3: Non-Generic Distinguisher

1. Make a list of 1000 different statistics you can compute about a given cipher.
2. Compute *each* of these for a given block X.
3. Build the distinguisher from the statistic which gives the most significant result.

Example 3: Non-Generic Distinguisher

We expect to find a statistic with a significance level of 1 in 1000.

This distinguisher can be applied to any individual cipher hence it is non-generic.

Computational Indistinguishability of Block Ciphers

What we are looking for usually is not perfect indistinguishability – it is only **computational indistinguishability**. We wish to be unable to distinguish between a block X and an ideal block cipher given a predetermined amount of limited computational resources.

References

- `https://www.tutorialspoint.com/cryptography/block_cipher.htm`
- *Cryptography Engineering* sections 3.3, 3.4
  By Ferguson, Schnier, and Kohno