Paper title and authors; where appeared.

Katz and Lindell, *Introduction to Modern Cryptography*

What is the main problem this paper attacks?

They construct a fixed length encryption scheme that is Choosen-Plaintext-Attack secure (for arbitrary length messages). A deterministic function cannot be used as it will necessarily have detectable patters. Thus, the key is to design a probabilisitc

What solution does the paper propose?

The they propose using a randomly generated "pad" value with each encryption and XORing it with the plaintext before encryption, destroying key-message relations

What central idea did the authors use to solve it?

They use the fact that pseudorandom pad is independent of both the key and plaintext, so it does not give information about either, and can be released freely. It serves only to make gaining information about subsequent encryptions of the same message impossible.

What is a weakness or limitation of the paper?

In order to be properly Choosen-Plaintext-Secure for arbitrary-length messages, the ciphertext has 2X blowup. That is, it is at least twice as large as the original message, making communication and storage cumbersome

Why is this paper important?

The ability to produce secure encryption for *arbitrary* length messages in Probabilistic Polynomial Time is very important, as the length messages typically sent across networks are not usually statically known at time of protocol creation, but must be dynamically determined during runtime. All things considered, 2X blowup isn't a terrible price for indistinguishable security, and it may be reduced further in a future construction.