- asymmetric
- encryption - symmetric
- hash function
- random #s
- numbers
- everything is a cryptographic concept
- Each message
  - Hash
  - Each hash is unique
- Keccak's primary advantage
- Ciphertext uniqueness can be leveraged
- Do not lose ciphertext
- At F_trajectory and above
Security

Key

 cry (p, k)

cry (p, k)

Input - Crypto - Output

Crypto must be open

Kerckhoff’s Principle - 1883
Large numbers

\[ \begin{array}{c}
15
\end{array} \]
Choose a random number...

L < random # <= max

L <= 128 bit or more

L <= largest #, chosen at random

Rounded # <= (ceiling)
5. Copy the same pseudo code for aeskeygen

\[
\begin{align*}
&n_3 \\ & \rightarrow \\ & n_2 \\ & \rightarrow \\ & \{n \leftarrow \text{SecKey} \} \\
& \rightarrow \\
& \text{Virtual key} \leftarrow \text{pseudo random} \rightarrow \text{secret key} \\
& \text{Compute random #5}
\end{align*}
\]
$n > n$

$\leq 2^{m-n}$

# of connections for each output

$m \leq n$

Input

Output

Each row
24. MD-5, SHA, SHA-256

important

Let us assume a kind of encoding -

 grues on input

 as a collection of

 compare hash function
fun Dec

decrypt

key [N]

[plaintext]

Encrypt

[plaintext]

Encrypt

[N] input

Symphony

one way function

one way function
Assym Encrypthon

$K_1 \rightarrow K_2$

$K_2$ is not derivable from $K_1$

Plain $\rightarrow$ cipher

$\rightarrow$ cipher

$\rightarrow$ plain
(Suggest this before a decision is made.)

Suggest building a summary of the plan presented.

Understand the redundancy in the decision-making process.

As complete an inventory as possible.

Be aware that key afterthoughts can impact the decision-making process.

Building a strong cider

Presentation