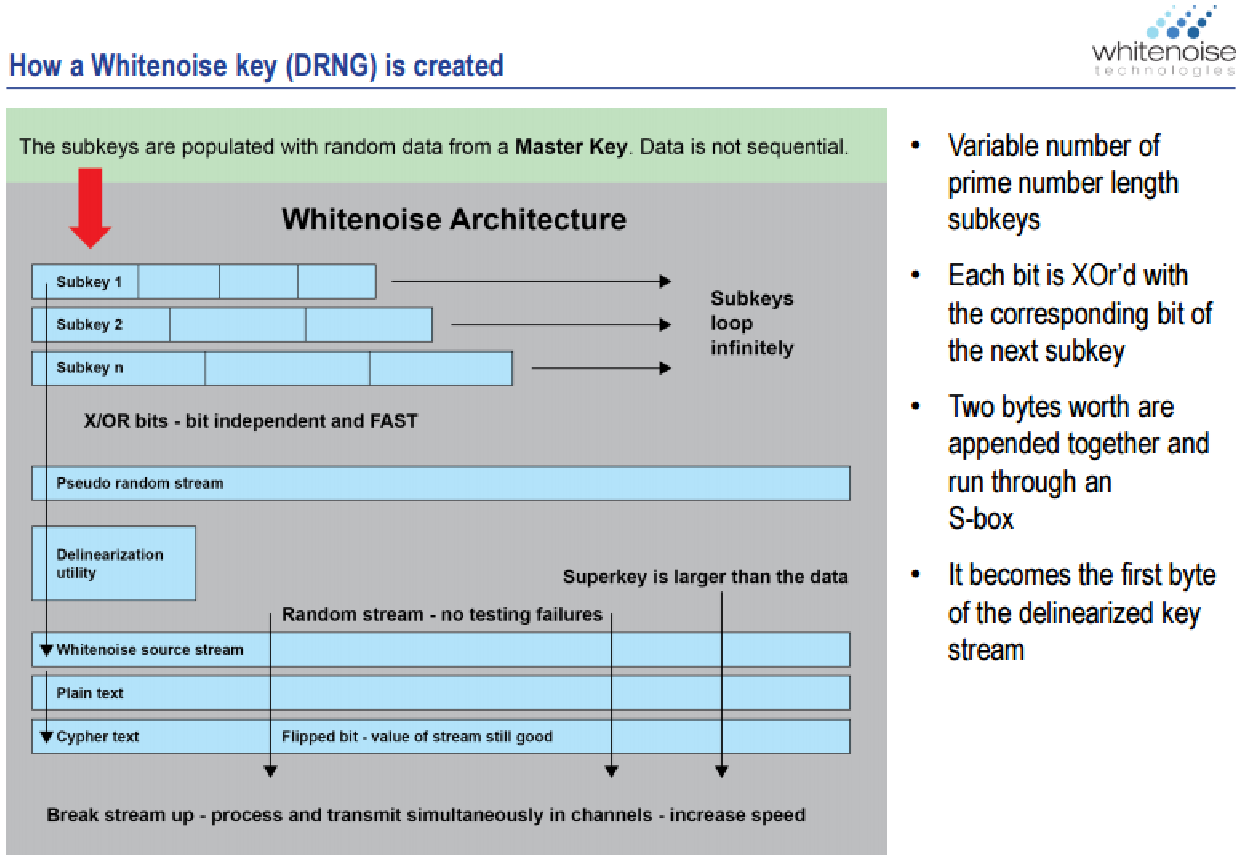
This is how a Whitenoise key is made

A Whitenoise key is comprised of a variable number of prime number length subkeys that are populated with random data. Each corresponding bit is XOr'd between subkeys to create a deterministic but random key. Only the subkey structure and offsets need to be saved to recreate this key.

As seen in the graphic below the smallest key that can be made by Whitenoise using the smallest prime number length subkeys is 110 billion bytes long and is greater than 1600 bits in strength. Note this is not the size of the subkeys on the master key.



How a Whitenoise key (DRNG) is created

The subkeys are populated with random data from a **Master Key**. Data is not sequential.

Whitenoise Architecture
Subkey 1
Subkey 2
Subkey n
Subkeys loop infinitely
X/OR bits - bit independent and FAST
Pseudo random stream
Delinearization utility
Superkey is larger than the data
Random stream - no testing failures
Whitenoise source stream
Plain text
Cypher text
Flipped bit - value of stream still good
Break stream up - process and transmit simultaneously in channels - increase speed

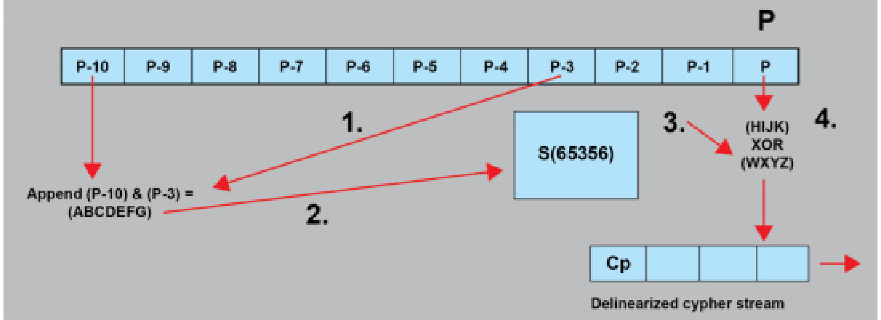
- Variable number of prime number length subkeys
- Each bit is XOr'd with the corresponding bit of the next subkey
- Two bytes worth are appended together and run through an S-box
- It becomes the first byte of the delinearized key stream

The subkeys loop infinitely left to right. We can use this data source only to the point where all the seams between all the subkeys line up perfectly vertically.

Whitenoise one-way functions

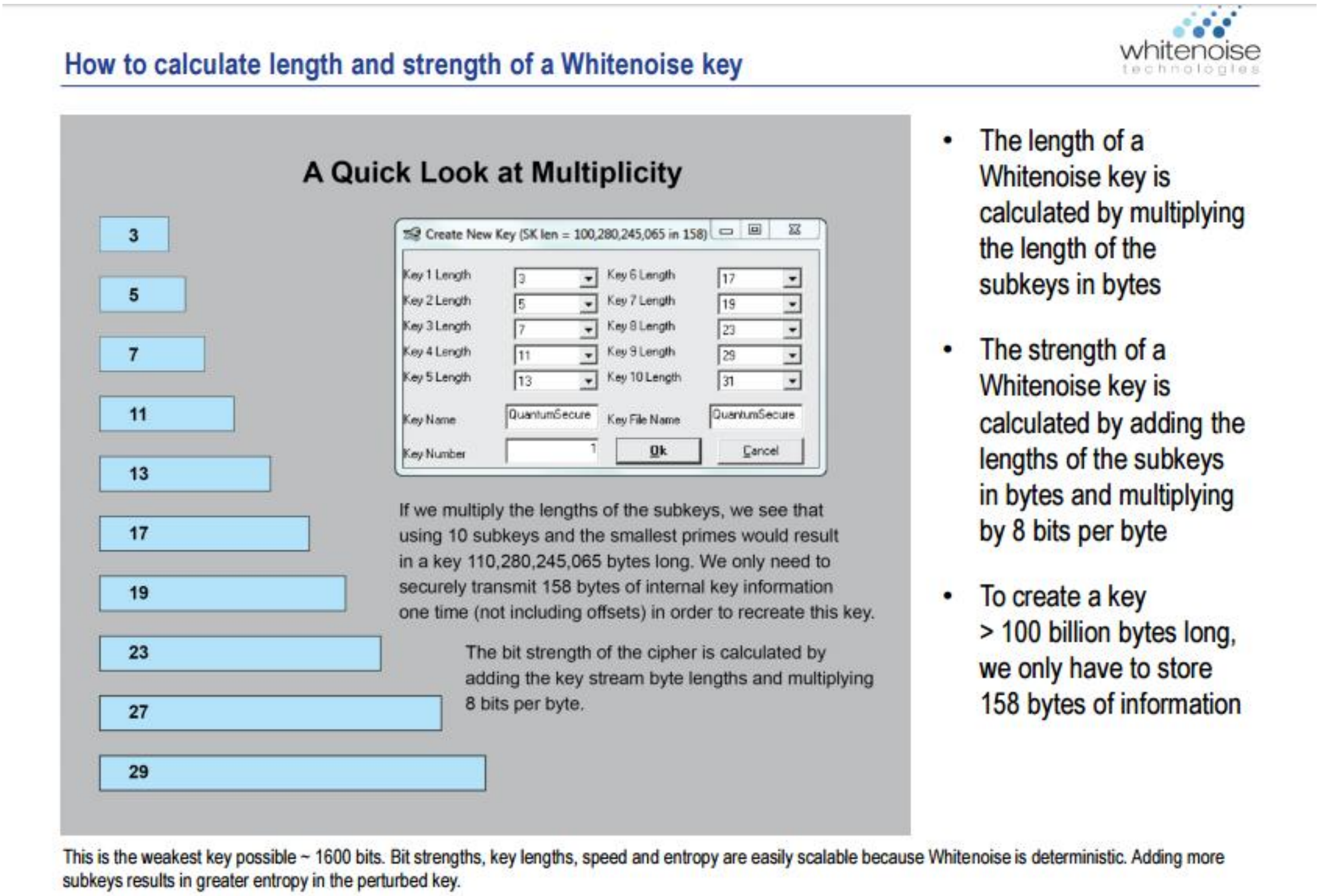
Whitenoise Delinearization

- ✔ Each box represents one byte
- ✔ P is the byte addressed by our offset point (the first byte in this example)
- ✔ The address P-3 is a co-prime distance of 3 bytes away from P.
- ✔ The address P-10 is an additional co-prime distance of 7 bytes away from P-3



The hacker has no knowledge of the master key which populates the subkeys with random data.

- Two bytes are taken from the initial key stream, appended together, and pushed through an S-Box
- Only one byte emerges
- A hacker cannot go backwards and guess two bytes of key stream from one byte of captured information
- The hacker has no knowledge of the number of subkeys, their lengths, or the random data they are populated with
- It is a one-time pad



How to calculate length and strength of a Whitenoise key

A Quick Look at Multiplicity

Create New Key (SK len = 100,280,245,065 in 158)

Key 1 Length	3	Key 6 Length	17
Key 2 Length	5	Key 7 Length	19
Key 3 Length	7	Key 8 Length	23
Key 4 Length	11	Key 9 Length	29
Key 5 Length	13	Key 10 Length	31
Key Name	QuantumSecure	Key File Name	QuantumSecure
Key Number	1		

If we multiply the lengths of the subkeys, we see that using 10 subkeys and the smallest primes would result in a key 110,280,245,065 bytes long. We only need to securely transmit 158 bytes of internal key information one time (not including offsets) in order to recreate this key.

The bit strength of the cipher is calculated by adding the key stream byte lengths and multiplying 8 bits per byte.

- The length of a Whitenoise key is calculated by multiplying the length of the subkeys in bytes
- The strength of a Whitenoise key is calculated by adding the lengths of the subkeys in bytes and multiplying by 8 bits per byte
- To create a key > 100 billion bytes long, we only have to store 158 bytes of information

This is the weakest key possible ~ 1600 bits. Bit strengths, key lengths, speed and entropy are easily scalable because Whitenoise is deterministic. Adding more subkeys results in greater entropy in the perturbed key.

If we were to add two subkeys of 31 and 37 bytes the length of the superkey, the strength of the key, and the entropy would increase dramatically:

In this example we added the underlined subkey lengths of 31 and 37 bytes.

The length of the key stream is determined by multiplying the lengths of the subkeys together.

The key is now 31 X 37 X 110,280,245,065 = 126,491,441,089,555 bytes long.

The key strength of the key is the sum of the subkey lengths times 8 bits per byte.

(3 + 7 + 11 + 13 + 17 + 19 + 23 + 27 + 29 + 31 + 37 bytes) times 8 bits per byte =

397 X 8 bits per byte = 3176 bit strength

Note: stream ciphers are inherently 10X stronger than block ciphers.

http://www.wnlabs.com/pdf/How_is_a_key_made.pdf