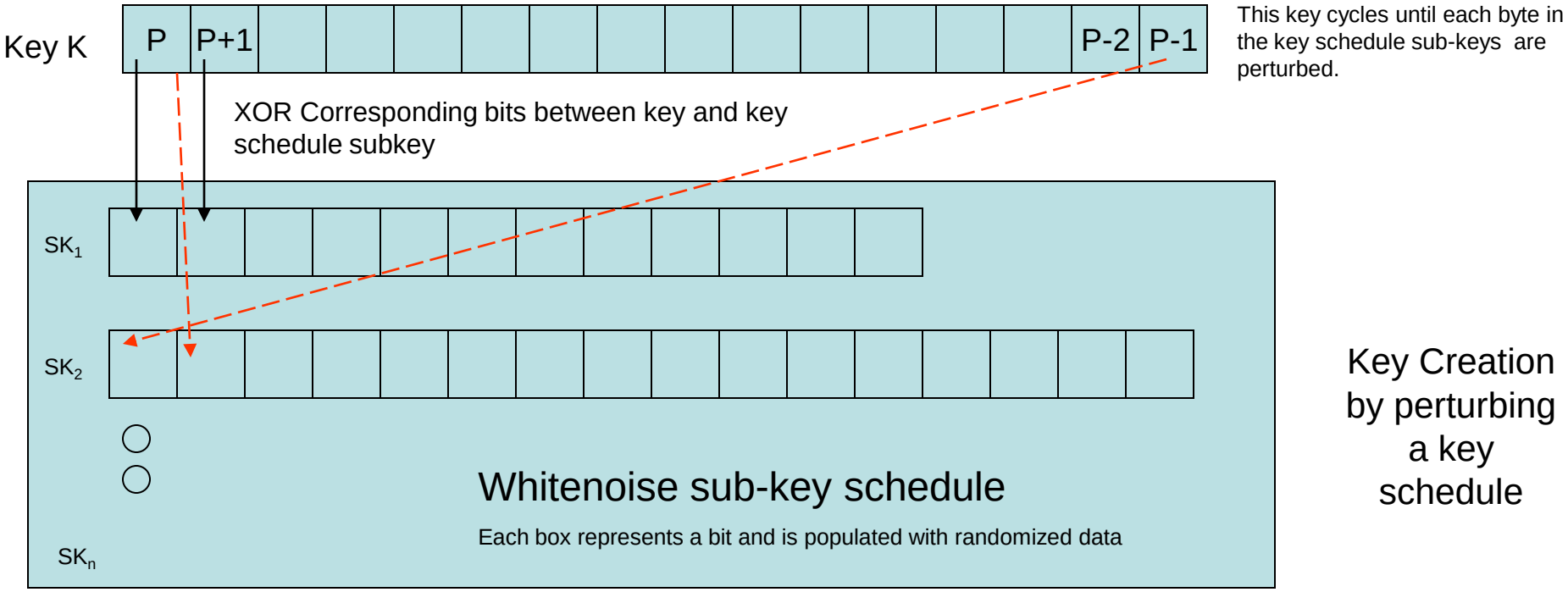
In the Email Attachment Encryptor a user enters two pass phrases which have previously been shared with a recipient by conversation, a separate email or on the telephone . These pass phrase keys are converted to hexadecimal values which are then used to perturb a key schedule to create a unique key with completely different output.



Process

Offsets are independent of key creation. For encryption use, the offset is managed by the application to prevent re-use of key segments. For identity management, detection and the use of DIVA, the offset is determined by process or formula from the distributed key K values.

- Starting at the offset P, XOR the corresponding bits of the first pass phrase key K and Sub-Key 1 (SK_1) until the sub-key is completely processed
- After SK_1 is perturbed, shift to the right and beginning at P-1 SK_2 is processed in the same fashion until completed
- After SK_2 is perturbed, shift to the right and beginning at P-2 SK_3 is processed in the same fashion until completed
- Repeat until all SKn keys are perturbed in this fashion
- Repeat process with second pass phrase

You have now created a unique, unbreakable Whitenoise key from two pass phrases and perturbed the sub-key structure schedule. The key stream that will be used is created by XOR'ing corresponding bits of SK_1 through SK_n (vertically) starting at a different offset. See Whitenoise schematics for key generation process.

A performance result from this process is the ability to create enormous, highly-random key streams while minimizing the footprint/storage required on the device or endpoint. It also minimizes the amount of key information that needs to be transmitted to the smaller sized keys in use today. It is particularly useful when security products are manufactured in foreign countries and one wants to eliminate that risk.