Foundations of Computer Security

Lecture 43: Transposition Ciphers

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Transposition Ciphers

A *transposition cipher* hides information by reordering the symbols in a message. The goal of transposition is *diffusion*.

Example: *Columnar transposition* involves writing the plaintext characters in a number of fixed length rows such as the following:

c_1	c_2	c_3	c_4	c_5
c_6	c_7	c_8	c_9	c_{10}
c_{11}	c_{12}	etc.		

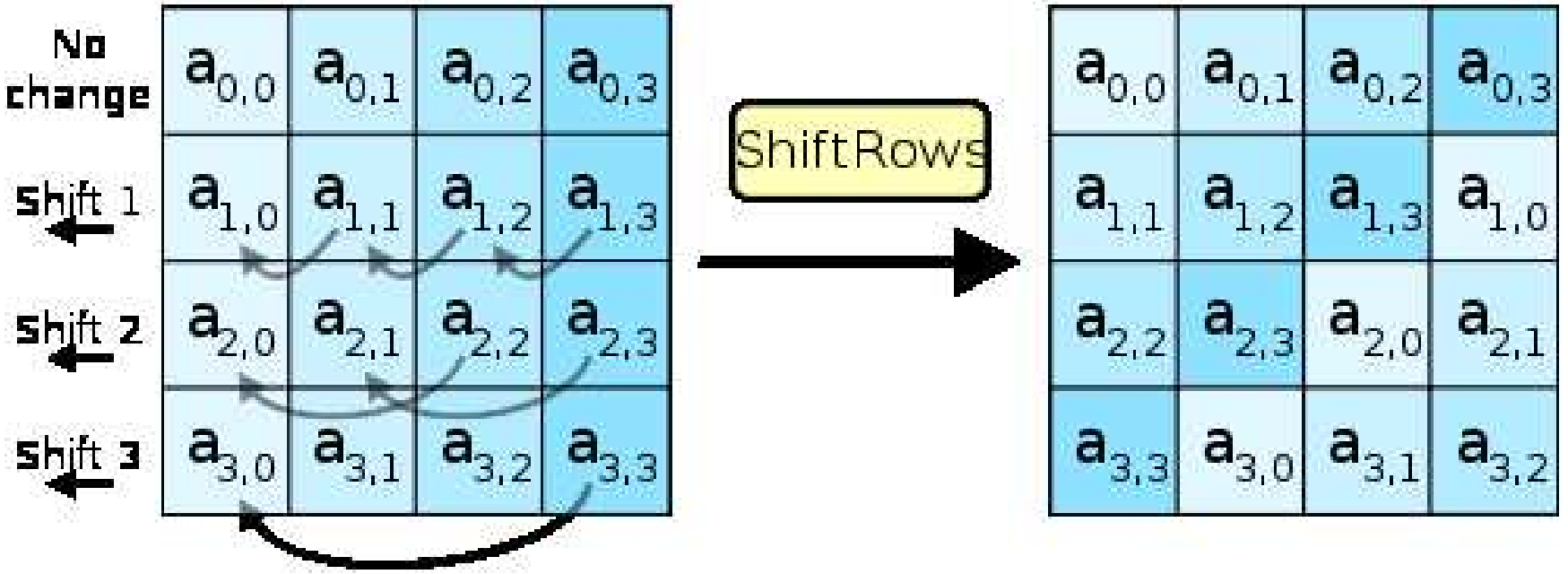
Form the ciphertext by reading down the columns: $c_1 c_6 c_{11} c_2 \ldots$.

If the message length is not a multiple of the number of columns, pad the final row with any character.

AES Transposition Step

Transposition need not only apply to symbols in a text.

The Advanced Encryption Standard (AES) contains a transposition step that reorders the bytes in a 16-byte array.



Cryptanalysis of Transpositions

Question: Given a text you believe to be the encryption of a text by transposition. How could you increase your confidence that that's the case?

Answer: Since transposition reorders characters, but doesn't replace them, the original characters still occur in the result. Letter frequencies are preserved in the ciphertext, but the frequencies of digrams, trigrams, etc. are not.

In a columnar transposition with rows of length n, adjacent characters in the plaintext are c_1 and c_{n+1}, c_2 and c_{n+2}, etc. Hypothesize a distance of n and try a decryption; if it fail, try a distance of $n + 1$, etc.

Combinations of Approaches

Substitutions and transpositions can be regarded as building blocks for encryption. Many important commercial algorithms use combinations of these.

A combination of two or more ciphers is called a *product cipher* or *cascade cipher*:

$$E_2(E_1(P, k_1), k_2)$$

A combination is not necessarily stronger than either cipher individually. It may even be weaker.

Lessons

- Transposition is another important building block for encryption.
- Because it preserves the symbols of a text, transposition preserves letter frequencies but not digrams, trigrams, etc.
- A product cipher is the combination of two or more encryption steps.

Next lecture: Symmetric vs. Asymmetric Encryption