**RC2** – szyfr blokowy z kluczem o zmiennej długości.

Wielkość bloku wynosi 8 bajtów (64 bity). Oznacza to, że dane wejściowe są najpierw dzielone na ośmiobajtowe bloki, z których każdy jest potem przetwarzany oddzielnie.

Każdy blok danych składa się z czterech 16-bitowych słów. Tablica czterech słów jest przedstawiana następująco: R[0] R[1] R[2] R[3]. Zarówno proces szyfrowania jak i deszyfrowania otrzymują jako dane wejściowe taką tablicę czterech słów, którą następnie modyfikują. Wynik działania tych operacji zapisywany jest w tej samej tablicy.

Oprócz danych do przetworzenia, szyfr RC2 otrzymuje również sekretny klucz szyfrujący, dostarczony przez użytkownika. Klucz może mieć różną wielkość, od jednego do 128 bajtów.

Operacje matematyczne przeprowadzane na kluczu operują zarówno na pojedynczych bajtach, jak i na całych słowach. Wobec tego, liczby zapisane w kluczu mogą być przedstawiane albo jako 64 dwubajtowe słowa: K[0], K[1], ..., K[63] albo jako 128 oddzielnych bajtów: L[0], L[1], ..., L[127].

Należy zauważyć, że każda część klucza może być zaadresowana zarówno za pomocą bajtów, jak i słów. Można zdefiniować poniższą zależność: K[i] = L[2·i] + 256·L[2·i+1]. Mniej znaczące osiem bitów każdego słowa znajduje się przed bardziej znaczącym bajtem.

**Szyfrowanie**

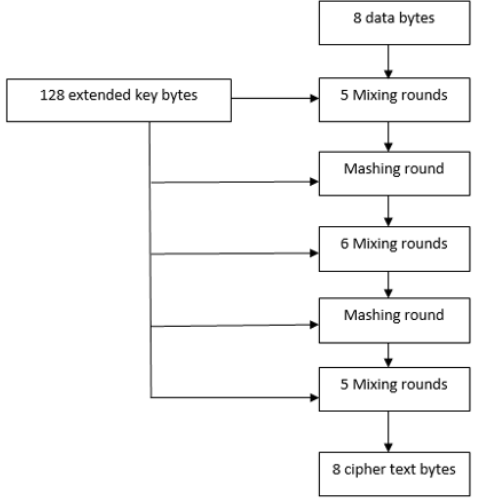
Procedura szyfrowania pobiera jako wejście cztery słowa: R[0] R[1] R[2] R[3], które składają się na jeden blok danych. Każdy blok zostanie zaszyfrowany przy pomocą takich samych 64 słów rozszerzonego klucza szyfrującego: K[0] K[1] ... K[63].

Aby zaszyfrować każdy blok danych, należy wykonać następujące kroki:

* Zainicjować licznik j na 0.
* Wykonać pięć rund Mixing.
* Wykonać jedną rundę Mashing.
* Wykonać sześć rund Mixing.
* Wykonać jedną rundę Mashing.
* Wykonać pięć rund Mixing.

Każda runda Mixing używa 4 bajtów klucza, wobec tego wszystkie 128 bajtów klucza są wykorzystywane podczas szyfrowania jednego bloku danych. Runda Mashing wykorzystuje bajty klucza w bardziej nieprzewidywalny sposób.

Podczas każdej rundy Mixing wykonywane są cztery operacje Mixing, przeprowadzane na czterech słowach bloku danych:

Schemat Blokowy Szyfrowania RC2

**Operacja Mixing:**

Operacja Mixing modyfikuje jedno słowo danych oraz zwiększa licznik j podczas procesu szyfrowania.

<<< - to jest rotacja bitów w lewo

>>> - rotacja bitów w prawo.

Trzy poniższe operacje są przeprowadzone podczas Mixing:  
    R[i] = R[i] + K[j] +  
         + (R[(i+4-1) mod 4] & R[(i+4-2) mod 4])  
         + ((~R[(i+4-1) mod 4]) & R[(i+4-3) mod 4])  
    j = j + 1  
    R[i] = R[i] <<< s[i]

**Operacja Mashing:**

Następujące działanie jest przeprowadzane podczas Mashing:  
    R[i] = R[i] + K[R[(i+4-1) mod 4] & 63]

**Deszyfrowanie:**

Procedura deszyfrowania pobiera jako wejście cztery słowa: R[0] R[1] R[2] R[3], które składają się na jeden blok szyfrogramu. Każdy blok zostanie odszyfrowany przy pomocą takich samych 64 słów rozszerzonego klucza: K[0] K[1] ... K[63].

Aby odszyfrować każdy blok szyfrogramu, należy wykonać następujące kroki:

* Zainicjować licznik j na 63.
* Wykonać pięć rund R-Mixing.
* Wykonać jedną rundę R-Mashing.
* Wykonać sześć rund R-Mixing.
* Wykonać jedną rundę R-Mashing.
* Wykonać pięć rund R-Mixing.

Podczas każdej rundy R-Mixing wykonywane są cztery operacje R-Mixing, przeprowadzane na czterech słowach bloku szyfrogramu. Podczas każdej rundy R-Mashing wykonywane są cztery operacje R-Mashing, przeprowadzane na czterech słowach bloku szyfrogramu.

**Operacja R-Mixing:**

Operacja R-Mixing modyfikuje jedno słowo szyfrogramu oraz zmniejsza licznik j podczas procesu deszyfrowania.

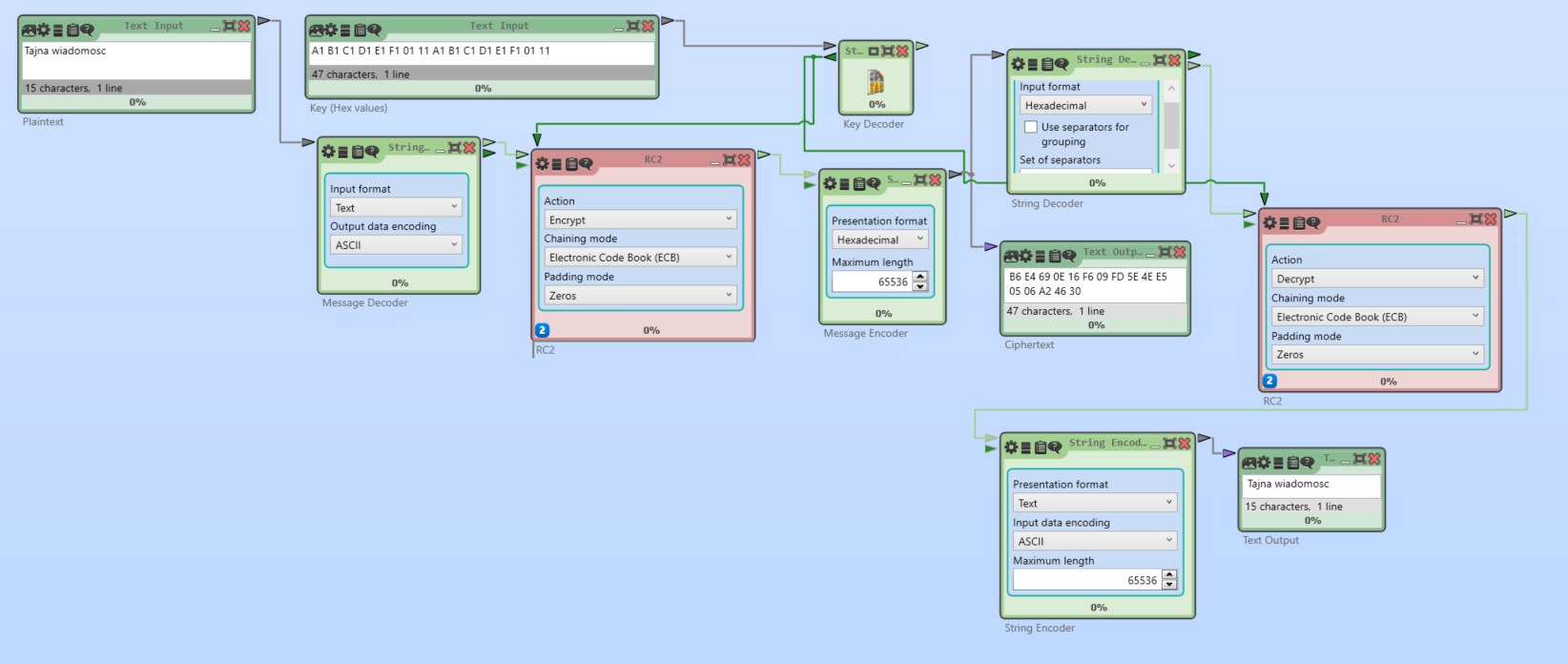
Trzy poniższe operacje są przeprowadzone podczas R-Mixing:  
    R[i] = R[i] >>> s[i]  
    R[i] = R[i] - K[j]  
         - (R[(i+4-1) mod 4] & R[(i+4-2) mod 4])  
         - ((~R[(i+4-1) mod 4]) & R[(i+4-3) mod 4])  
    j = j - 1  
  
gdzie j oznacza zmienną licznika

**Operacja R-Mashing:**

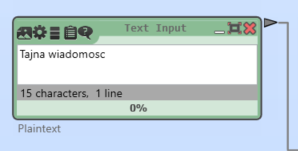
Operacja R-Mashing modyfikuje jedno słowo szyfrogramu podczas procesu deszyfrowania.

Następujące działanie jest przeprowadzane podczas R-Mashing:  
    R[i] = R[i] - K[R[(i+4-1) mod 4] & 63]

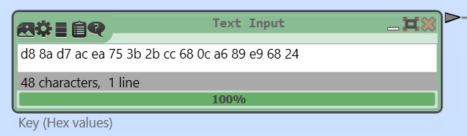
**Cały wygląd realizacji szyfrowania I rozszyfrowania**



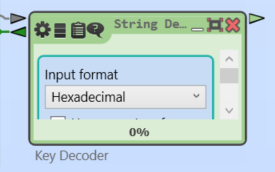
Dla szyfrowania mamy tekst (Tajna wiadomosc):



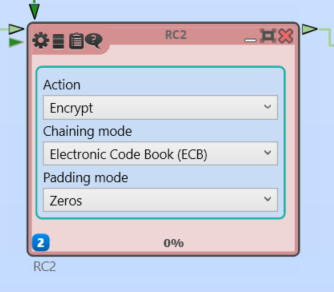
Dalej mamy klucz z losowych 16 bajt:



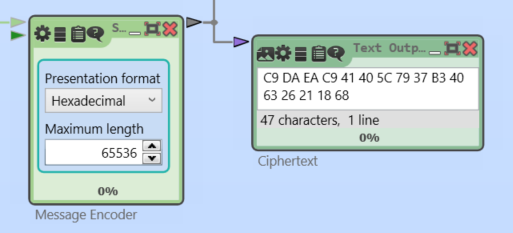
Dalej tekst klucza przetwarzamy w hex format:



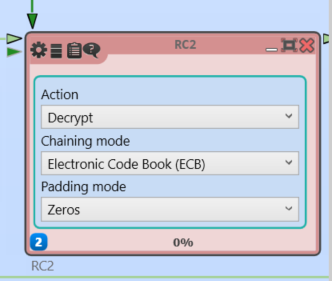
Dalej włączymy klucz w HEX formacie z tekstem, który chcemy zaszyfrować.



Po skończeniu szyfrowania otrzumujemy ciąg bajt w formacie HEX

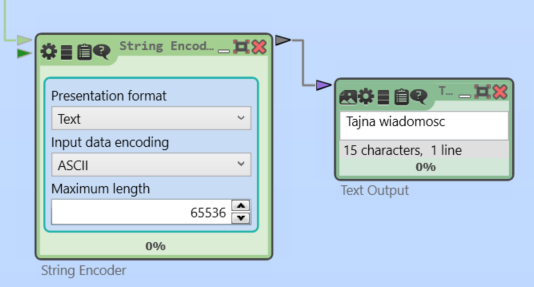


Dla deszyfrowania otrzymany ciąg HEX przetwarzamy w tekst I włączymy do RC2 deszyfrowania.

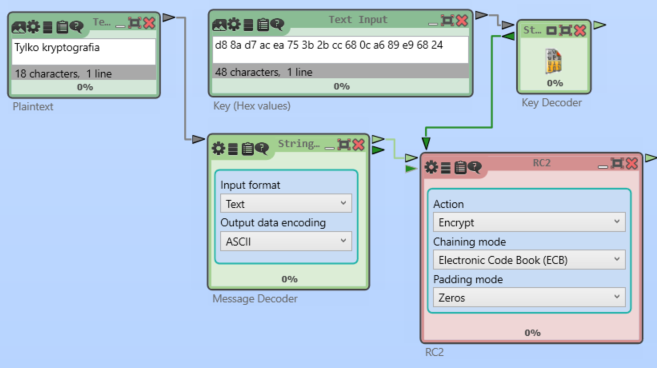


Wybieramy opcję deszyfrowania.

Dowłączamy klucza (którego używaliśmy do szyfrowania).

Otrzymujemy ciąg HEX, który musimy przetwarzyć w tekst.

Analogicznie robimy dla tekstu “Tylko kryptografia”



I otrzymujemy wynik w formie HEX znaczeń.

