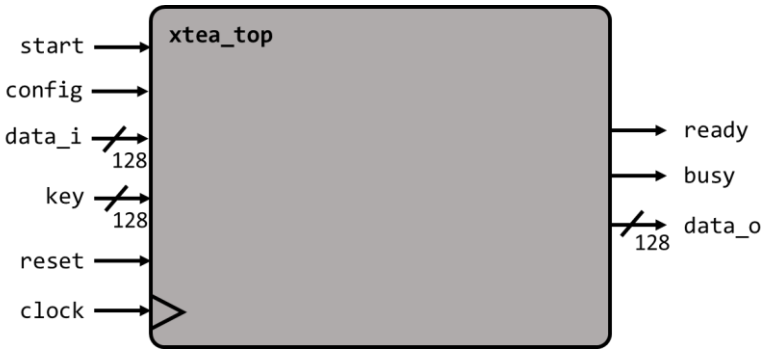
TRABALHO 4: MÓDULO DE CRIPTOGRAFIA (XTEA)

1. OBJETIVO

O **objetivo** desse trabalho é fazer um protótipo de um módulo de criptografia usando como referência um programa em linguagem C. Note que esse trabalho deverá ser realizado de forma **individual ou em dupla**. Ademais, este trabalho pode ser desenvolvido em **Verilog** ou **VHDL**.

2. ESPECIFICAÇÃO DO MÓDULO DE CRIPTOGRAFIA

A Figura abaixo mostra a entidade do módulo de criptografia, **`xtea_top`**, isto é, suas portas de entrada e saída. Note que o algoritmo de criptografia a ser implementado é o **XTEA**, o qual suporta um tamanho de mensagem de 128 bits (`data_i`) e um tamanho de chaves de 128 bits (`key`), e devolve uma mensagem de 128 bits (`data_o`) que pode estar criptografada ou descriptografada, dependendo da operação solicitada. A operação é definida pelo sinal (`config`), onde a operação de encriptar é '`1`' e decriptar é '`0`'. Além disso, o sinal `start` indica o início da criptografia, o sinal `busy` indica que o módulo está em operação. Por fim, o sinal `ready` é colocado em nível lógico alto durante um ciclo de *clock* para indicar que a mensagem está pronta (isto é, válida) na porta `data_o`.



Primeiramente você deve entender o algoritmo de criptografia **XTEA**, o qual é oferecido uma referência em linguagem C. Após o estudo do algoritmo **XTEA**, você deve **especificar uma máquina de estados (FSM) para encriptação e outra para decriptação além de um módulo superior que controla ambos os módulos.**

ENTREGA

A data da entrega deste trabalho é indicada no Moodle. E deve-se enviar um arquivo compactado (formato **.zip**) com os seguintes arquivos:

A pasta do projeto que contenha:

- O módulo **`xtea_top(.v/.vhd)`** composto (no mínimo) dos seguintes submódulos:
  - **`xtea_dec(.v/.vhd)`** – responsável pelo processo de decriptação
  - **`xtea_enc(.v/.vhd)`** – responsável pelo processo de encriptação
- Um **testbench** – com no mínimo 10 casos de teste de criptografia e descriptografia. Instrumentalize o modelo fornecido em *software* para gerar os casos de teste.
- O *script* de simulação para validação do projeto no Modelsim/Questasim também deve estar presente!

AVALIAÇÃO

- **[3 pontos]** Implementação da encriptação;
- **[3 pontos]** Implementação da decriptação;
- **[3 pontos]** *Testbench* e simulação demonstrando o funcionamento do circuito (pelo menos 10 casos de testes devem ser utilizados);
- **[1 ponto]** Organização e qualidade do código.

A não implementação das funções de encriptação/decriptação em módulos separados irá implicar em desconto de 50% na nota de cada módulo.