





The Merkle-Hellman Cryptosystem







ALGORITMOS E
ESTRUTURAS DE DADOS 2021
Prof. Tomás Silva

Daniel Ferreira – 102442 – 33.3% Guilherme Antunes – 103600 – 33.3% Pedro Rasinhas – 103541 – 33.3%

ÍNDICE

Introdução
The Merkle-Hellman Cryptosystem
Abordagem
Brute Force
Clever Brute Force
Horowitz and Sahni
Schroeppel and Shamir
Resultados e algumas conclusões
Comparação Brute Forces
Comparação Horowitz and Sahni e Schroeppel and Shamir
Comparação de todos os métodos, em todos os PCs
Conclusões Finais
Soluções
Solução 102442_extra.h
Solução 103541_extra.h
Solução 103600_extra.h
Código - C
Brute Forces
Horowitz and Sahni
Código - MATLAR

Introdução

The Merkle-Hellman Cryptosystem

O objetivo deste trabalho prático foi implementar e estudar o comportamento de diversas técnicas de resolução do sistema de criptografia de Merkle e Hellman.

Este sistema consiste num problema de soma de subconjuntos oculto numa sequência de números inteiros positivos em que a mensagem secreta é uma sequência binária em que os uns denotam a contribuição do número nesse índice para a soma desejada (a mensagem encriptada, disponibilizada) e os zeros a não contribuição.

Por exemplo, para um problema de tamanho 6, em que a soma do primeiro e terceiro elementos da lista de números corresponde à soma desejada, a solução seria 10100.

O trabalho desenvolvido baseia-se num conjunto destes problemas: 20 valores aos quais se tentam chegar a partir duma lista de tamanho *n*, variando de 10 até 64.

Abordagem

Recorrendo a diversos algoritmos, exploraram-se as técnicas computacionais mais eficientes e mais céleres para a resolução deste sistema.

Nomeadamente, utilizámos e comparámos 4 algoritmos de diversos níveis de complexidade computacional:

- Brute Force
- Clever Brute Force
- Horowitz and Sahni
- Schroeppel and Shamir

A *Brute Force* e a *Clever Brute Force* são funções recursivas que abordam o problema duma forma mais simplista do ponto de vista do programador, mas que aumentam a complexidade do problema do ponto de vista computacional.

A Horowitz and Sahni e a Schroeppel and Shamir baseiam-se na técnica de meet-in-the-middle que resulta numa drástica redução da complexidade computacional da resolução deste problema já que reduz o número de somas a efetuar, sendo essa a parte do problema mais laboriosa e demorada, tornando assim a sua resolução mais ágil e possibilitando a resolução de problemas com um valor de n significativamente mais elevado, face às funções recursivas descritas anteriormente.

Brute Force

Como referido anteriormente, a primeira abordagem foi escolhida com base na simplicidade da sua implementação, recorrendo-se assim a uma função recursiva. Em contrapartida, a sua complexidade computacional não é reduzida devido à falta de otimizações.

No método Brute Force, o *array* de números é percorrido e são efetuadas todas as possíveis somas. Para cada elemento do *array* e para cada possível soma, é gerado um *bit vector* em que um 1 representa a contribuição do elemento do *array* nesse índice para essa dada soma e um 0 a não contribuição, tal como na descrição do problema. Caso a soma obtida corresponda à soma desejada (mensagem encriptada do problema), o programa termina e devolve o *bit vector* correspondente. O programa também termina caso não encontre a soma desejada.

Durante o processo de execução, a função apenas descarta o subconjunto atual que está a ser utilizado para obter a soma (conhecido como **ramo**) quando esgotar todos os elementos ainda disponíveis e ainda não tiver encontrado a soma desejada.

Devido à natureza abrangente deste método, revela-se pouco eficiente, tendo uma complexidade computacional de $O(n^2)$.

Clever Brute Force

Como o nome indica, a função Clever Brute Force é uma versão otimizada do método Brute Force anteriormente referido, recorrendo à técnica de *branch-and-bound*.

Adaptando uma das funcionalidades da função anterior, o facto de descartar o **ramo** quando esgotasse o número de elementos possíveis de somar, este método expande o número de critérios em que este corte ocorre, diminuindo assim o número de somas a efetuar, levando a uma maior eficiência.

Nomeadamente, abandona-se o **ramo** atual quando a soma obtida exceder a soma desejada ou quando a soma dos elementos ainda disponíveis for menor que a soma desejada, ou seja, há mudança de **ramo** quando se prova que é impossível atingir a soma desejada com a atual.

Para além disto, o *array* é percorrido de forma decrescente de modo a aumentar a probabilidade da soma no **ramo** atual exceder a soma desejada, desencadeando o processo acima descrito e minimizando o número de somas a efetuar, contribuindo ainda mais para a eficiência deste método.

Como se trata do mesmo método base de tentativa e erro, ocorrendo apenas um descarte marginal de casos a considerar, a complexidade computacional desta função é também de $O(n^2)$.

Horowitz and Sahni

Esta função utiliza a técnica de *meet-in-the-middle* que procura reduzir drasticamente a complexidade computacional do *subset sum problem*.

O conjunto de números da lista dada é dividido em dois *arrays* **ordenados** (recorreu-se ao *merge sort*) de tamanho aproximadamente igual.

Feita a divisão, calcula-se e guarda-se os valores de todas as somas possíveis de cada elemento noutros dois *arrays*, também eles **ordenados**, um com as somas do primeiro e outro com as somas do segundo, cada um correspondendo aos iniciais.

Partindo do facto que a soma de determinados números dum conjunto A pode ser obtida pela soma de outros que por sua vez resultam nos números contidos no conjunto A, percorrem-se ambos os *arrays* tentando encontrar o índice dos elementos, que somados, resultem na soma desejada.

Encontradas as posições dos elementos participantes, gera-se uma sequência binária de tamanho *n*, resultado da concatenação dos elementos participantes em ambos os *arrays*, seguindo a lógica do enunciado do problema: 1 para elemento participante e 0 para não participante.

De notar que este algoritmo representa um ganho de eficiência tremendo já que reduz a complexidade, face à função recursiva usada inicialmente, de $O(2^n)$ para $O(n^*2^{n/2})$.

Schroeppel and Shamir

Utilizando novamente a técnica do *meet-in-the-middle* construiu-se o algoritmo mais eficiente deste trabalho, o único que encontrou todas as soluções dos problemas dados, até n=64, sendo que o algoritmo anterior apenas atingiu o valor de n=57 com sucesso e os que se baseiam em força bruta, o valor de n=35.

A primeira diferença relativamente ao terceiro algoritmo é que nesta implementação a lista de números do problema é dividida em quatro partes ao invés de duas. Calculadas todas as somas possíveis de cada subconjunto, são ordenadas com recurso ao algoritmo *merge sort*.

Seguidamente, gera-se uma *min heap* e uma *max heap* cada um para dois subconjuntos, sendo os valores raíz a soma dos primeiros elementos dos dois subconjuntos e a soma dos últimos elementos dos outros dois subconjuntos, respetivamente.

Efetua-se a soma entre os valores descritos; caso seja superior à soma desejada, alterase a raíz da *max heap* para a maior soma seguinte, descartando a atual; caso seja inferior, descarta-se a raíz da *min heap* passando a utilizar a soma imediatamente superior, ou seja, utilizando o elemento seguinte de apenas uma das *heaps*, mantendo a utilização do primeiro da outra.

O programa termina quando a soma encontrada for igual à soma desejada.

De notar que as somas encontradas são geradas *on-the-fly*, permitindo assim uma redução substancial na memória utilizada.

Devido à maneira ponderada como este algoritmo foi elaborado, permite atingir valores de n não antes possíveis, já que resulta numa redução da complexidade computacional para $O(2^{n/2})$.

Resultados e algumas conclusões

Para se ter uma melhor noção de como o tempo de execução de cada algoritmo vai depender das especificações da máquina onde está a ser executado, decidimos executar os algoritmos em três computadores diferentes (com as suas especificações abaixo descritas).

Nas páginas seguintes vão ser apresentados diversos gráficos a demonstrar e a comparar os tempos de execução para as diferentes abordagens ao problema. Optámos por colocar um gráfico, para cada PC, a comparar as **Brute Forces** e um gráfico a comparar os algoritmos com a técnica *meet-in-the-middle* (*Horowitz and Sahni* e *Schroeppel and Shamir*). Dispusemos também dois gráficos a comparar a *performance* de todos os PCs, um para os dois primeiros algoritmos (**Brute Forces**) e outro para comparar a *performance* no terceiro e quarto algoritmos. Por fim, expusemos um último gráfico onde entram todos os algoritmos executados por todos os PCs, com o intuito de se visualizar claramente as diferenças significativas entre os métodos brutos (**Brute Forces**) e os métodos mais complexos (*Horowitz and Sahni* e *Schroeppel and Shamir*).

Computadores e as suas especificações:

	Memória RAM	Processador
PC1	16GB @3000 MHz CL15	Intel(R) Core(TM) i7-8700K CPU @3.70GHz 5.0 GHz
PC2	16GB @3200 MHz CL16	AMD Ryzen 7 4800HS @2.0 GHz 4.2 GHz
PC3	16GB @2667 MHz CL17	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz 2.20 GHz

Notas:

A falta de pontos nos gráficos do PC1 deve-se ao facto de o tempo de execução ser arredondado pelo wsl2 para 0 segundos, e, por conseguinte, o *MatLab* não considera esses valores para o *plot*.

No método Horowitz and Sahni o tempo que o programa leva a calcular os dois *arrays* de somas possíveis e a ordená-los é calculado apenas uma vez para cada *n e antes de estes arrays serem submetidos à comparação feita pelo método Horowitz até coincidir com a desired_sum.* Este tempo de somas e ordenação é somado no fim ao tempo médio e ao tempo máximo que cada soma levou. Decidimos proceder assim visto que seria uma perda de tempo executar esse processo 20 vezes para

cada <i>n, sendo que as arrays teriam sempre os mesmos valores,</i> o que provocaria um aumento dos tempos de execução.

Comparação Brute Forces

PC1

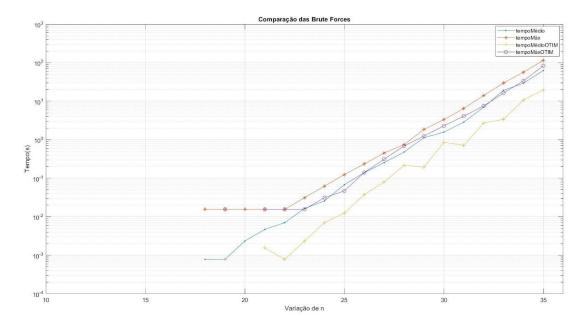


Figura 1 – Comparação dos métodos **Brute Forces** no PC1

PC 2

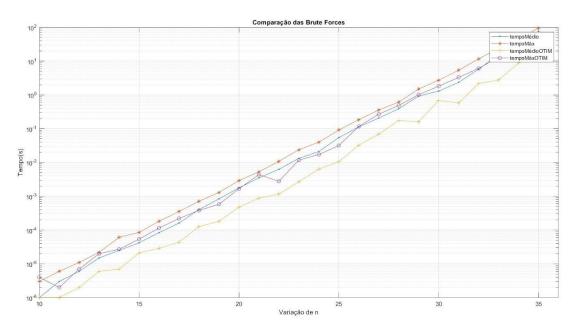


Figura 2 – Comparação dos métodos **Brute Forces** no PC2

PC 3

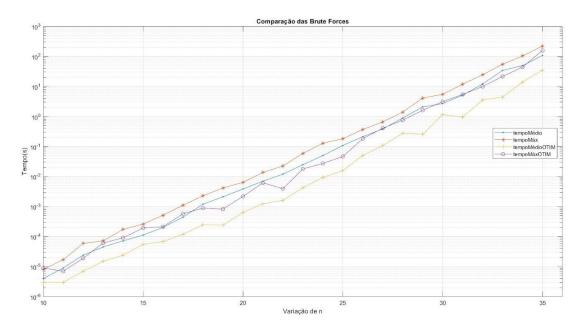


Figura 3 – Comparação dos métodos **Brute Forces** no PC3

Como se pode observar nos gráficos acima, a **Brute Force Otimizada** é significativamente mais rápida que a **Brute Force** não otimizada (como seria de esperar).

Três PCs

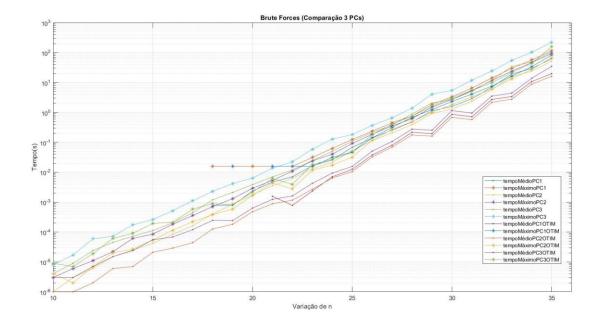


Figura 4 – Comparação dos métodos **Brute Forces** em todos os PCs

Comparação Horowitz and Sahni e Schroeppel and Shamir

PC1

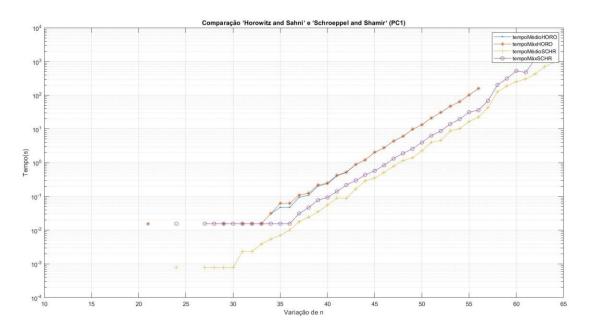


Figura 5 – Comparação dos métodos *Horowitz and Sahni e Schroeppel and Shamir* no PC1

PC2

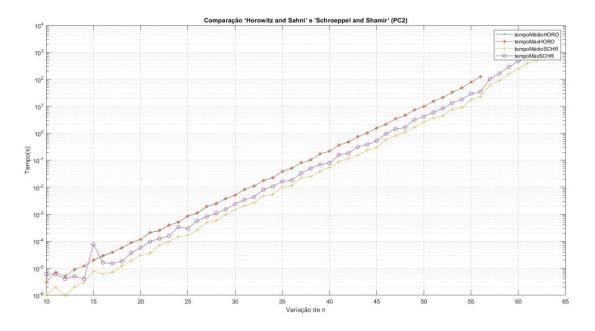


Figura 6 – Comparação dos métodos *Horowitz and Sahni e Schroeppel and Shamir* no PC2

PC 3

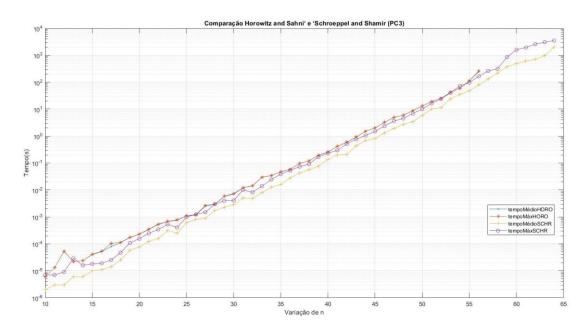


Figura 7 – Comparação dos métodos *Horowitz and Sahni e Schroeppel and Shamir* no PC3

Como se pode observar nos gráficos acima, a velocidade dos métodos *Horowitz and Sahni e Schroeppel and Shamir* é semelhante, porém este último permite alcançar *n* mais elevados.

Três PCs

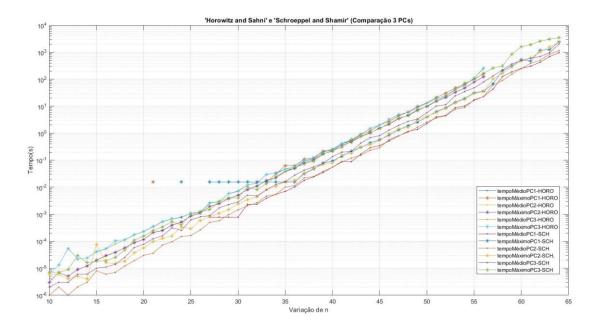


Figura 8 – Comparação dos métodos *Horowitz and Sahni e Schroeppel and Shamir* nos três PCs

Comparação de todos os métodos, em todos os PCs

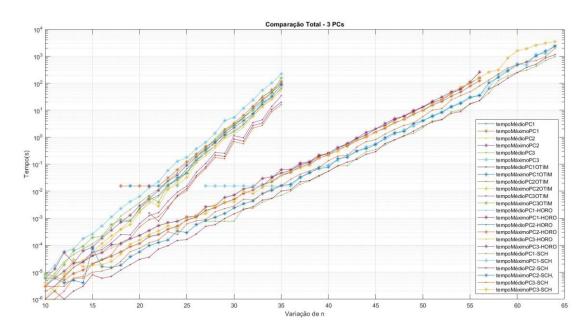


Figura 9 – Comparação de todos os métodos nos três PCs

Como esperado, o tempo de execução dos métodos *Horowitz and Sahni e Schroeppel and Shamir* é muito menor, quando comparado aos algoritmos de força bruta, permitindo também *ns* mais elevados.

Conclusões Finais

Em suma, este trabalho demonstrou que diferentes complexidades e diferentes capacidades computacionais irão originar tempos de execução diferentes e exigir tipos de abordagens diferentes, o que nos leva a concluir que na resolução de um problema é tão relevante a sua resolução como a decisão de qual abordagem seguir tendo em conta a complexidade do problema que nos é apresentado.

Soluções

Solução 102442_extra.h

n = 10

010111111011

n = 12

0011001111110

0000101011110 0111000011110 n = 13

11010111110000

n = 14 0010111100010111

Solução 103541_extra.h

Solução 103600_extra.h

Código - C

Brute Forces

```
id showbits(integer_t x, int total_bits)
   for (int i = total\_bits - 1; i >= 0; i--)
       putchar(x & (1u << i) ? '1' : '0');</pre>
void showbits2(integer_t x, int total_bits)
   for (int i = 0; i <= total_bits - 1; i++)
       putchar(x & (1u << i) ? '1' : '0');</pre>
int bruteforce_rec1(int n, integer_t *p, int currIdx, integer_t partialSum, integer_t desiredSum, integer_t mask, integer_t *comb)
   if (partialSum == desiredSum)
       *comb = mask;
    if \ (bruteforce\_rec1(n, \ p, \ currIdx + 1, \ partialSum + p[currIdx], \ desiredSum, \ (mask \ | \ (1 << currIdx)), \ comb)) 
       return bruteforce_rec1(n, p, currIdx + 1, partialSum, desiredSum, mask, comb);
 int bruteforce_rec2(int n, integer_t *p, int currIdx, integer_t partialSum, integer_t desiredSum, integer_t mask, integer_t *comb)
    if (partialSum > desiredSum)
    if (partialSum == desiredSum)
         *comb = mask:
         return 1;
    if (bruteforce_rec2(n, p, currIdx - 1, partialSum + p[currIdx], desiredSum, (mask | (1 << (currIdx))), comb))
         return bruteforce_rec2(n, p, currIdx - 1, partialSum, desiredSum, mask, comb);
```

```
main(void)
               unsigned int n = all_subset_sum_problems[i].n;
integer_t *p = all_subset_sum_problems[i].p;
double somaTempos = 0;
double tempoMaximo = 0;
                      integer_t desiredSum = all_subset_sum_problems[i].sums[j];
integer_t comb = 0;
                  print(
}
clse
{
    printf("\nSoluçao NÃO encontrada!\n");
}
    time = cpu_time() - time;
somaTempos == time;
if (time > tempoMaximo)
    tempoMaximo = time;
/ n_sums;
               double tempoMedio = somaTempos / n_sums;
printf("%d %f %f\n", i + 10, tempoMedio, tempoMaximo);
  if (func == 2)
                   unsigned int n = all_subset_sum_problems[i].n;
integer_t *p = all_subset_sum_problems[i].p;
double somaTempos = 0;
double tempoMaximo = 0;
                           integer_t desiredSum = all_subset_sum_problems[i].sums[j];
integer_t comb = 0;
                           double time = cpu time();
                                  showbits2(comb, n);
printf("\n");
                          }
time = cpu_time() - time;
somaTempos += time;
if (time > tempoMaximo)
tempoMaximo = time;
```

double tempoMedio = somaTempos / n_sums; printf("%d %f %f\n", i + 10, tempoMedio, tempoMaximo);

Horowitz and Sahni

```
void insertion_sort(integer_t *data, int first, int one_after_last, integer_t *bits)
{
    int i, j;
    for (i = first + 1; i < one_after_last; i++)
    {
        integer_t temp = data[i];
        integer_t temp2 = bits[i];
        for (j = i; j > first && temp < data[j - 1]; j--)
        {
            data[j] = data[j - 1];
            bits[j] = bits[j - 1];
        }
        data[j] = temp;
        bits[j] = temp2;
    }
}</pre>
```

```
void Merge(integer_t *data, int first, int one_after_last, integer_t *bits)
    int i, j, k, middle;
integer_t *buffer;
    integer_t *buffer2;
    if (one_after_last - first < 40)</pre>
       insertion_sort(data, first, one_after_last, bits);
       middle = (first + one_after_last) / 2;
        Merge(data, first, middle, bits);
        Merge(data, middle, one_after_last, bits);
        buffer = (integer_t *)malloc((size_t)(one_after_last - first) * sizeof(integer_t)) - first;
        buffer2 = (integer_t *)malloc((size_t)(one_after_last - first) * sizeof(integer_t)) - first;
        i = first;
        j = middle;
        k = first;
        while (k < one_after_last)
           if (j == one_after_last || (i < middle && data[i] <= data[j]))</pre>
                buffer2[k] = bits[i];
                buffer[k++] = data[i++];
                buffer2[k] = bits[j];
                buffer[k++] = data[j++];
        for (i = first; i < one_after_last; i++)</pre>
            data[i] = buffer[i];
            bits[i] = buffer2[i];
        free(buffer + first);
free(buffer2 + first);
```

```
void somas(int n, integer_t *vals, integer_t *sums, integer_t *bits)
       integer_t som, comb;
       for (integer_t a = 0; a < 1 << n; a++)</pre>
             som = 0;
              comb = 0;
              for (int i = 0; i < n; i++)
                    if (a & (1 \ll i))
                           som += vals[i];
                           comb = comb \mid (1 << i);
              sums[a] = som;
              bits[a] = comb;
nt horowitz(integer_t desired_sum, int sizeA, int sizeB, integer_t sumsA[], integer_t sumsB[], integer_t bitsA[], integer_t bitsB[], int nA, int nB)
  sums8 = &sums8[(int)size8 - 1];
bits8 = &bits8[(int)size8 - 1];
while (sumsA < &sumsA[(int)sizeA] || sums8 > &sumsB[0])
         sumsA++;
bitsA++;
         bitsB--;
     integer_t b = *bitsA | (*bitsB << nA);
for (int i = 0; i < nA + nB; i++)</pre>
        printf("%s", b & 1 ? "1" : "0");
b = b >> 1;
     printf("\n");
return 1;
```

```
int main(void)
    for (int i = 0; i < n_problems; i++)
             int n = all_subset_sum_problems[i].n;
             integer_t *p = all_subset_sum_problems[i].p;
             double somaTempos = 0;
            double tempoMaximo = 0;
             int nA = n / 2;
int nB = n - nA;
             p = all_subset_sum_problems[i].p;
             int sizeA = 1 << nA;</pre>
             int sizeB = 1 << nB;</pre>
             integer_t *sumsA = malloc(sizeA * sizeof(integer_t));
integer_t *sumsB = malloc(sizeB * sizeof(integer_t));
             integer_t *bitsA = malloc(sizeA * sizeof(integer_t));
             integer_t *bitsB = malloc(sizeB * sizeof(integer_t));
             double time2 = cpu_time();
             somas(nA, p, sumsA, bitsA);
             somas(nB, p + nA, sumsB, bitsB);
            Merge(sumsA, 0, sizeA - 1, bitsA);
Merge(sumsB, 0, sizeB - 1, bitsB);
             time2 = cpu_time() - time2;
             for (int j = 0; j < n_sums; j++)</pre>
                 integer_t desired_sum = all_subset_sum_problems[i].sums[j];
                 double time = cpu_time();
                 if (!horowitz(desired_sum, sizeA, sizeB, sumsA, sumsB, bitsA, bitsB, nA, nB))
                      printf("\nSoluçao NÃO encontrada!\n");
                 time = cpu_time() - time;
                 somaTempos += time;
                 if (time > tempoMaximo)
                      tempoMaximo = time;
            free(sumsA);
            free(sumsB);
            free(bitsA);
            free(bitsB);
            double tempoMedio = somaTempos / n_sums;
            printf("%d \%f \%f\n", i + 10, tempoMedio+time2, tempoMaximo+time2);\\
    return 0;
```

Schroeppel and Shamir

```
integer_t som;
    integer_t comb;
    int ind1;
   int ind2;
void insertion_sort(sum *data, int first, int one_after_last)
   for (i = first + 1; i < one_after_last; i++)</pre>
        sum temp = data[i];
        for (j = i; j > first && temp.som < data[j - 1].som; j--)</pre>
          data[j] = data[j - 1];
        data[j] = temp;
void Merge(sum *data, int first, int one_after_last)
    int i, j, k, middle;
    sum *buffer;
    if (one_after_last - first < 40)</pre>
        insertion_sort(data, first, one_after_last);
       middle = (first + one_after_last) / 2;
        Merge(data, first, middle);
        Merge(data, middle, one_after_last);
        buffer = (sum *)malloc((size_t)(one_after_last - first) * sizeof(sum)) - first;
        i = first;
        j = middle;
        while (k < one_after_last)</pre>
            if (j == one_after_last || (i < middle && data[i].som <= data[j].som))</pre>
                buffer[k++] = data[i++];
               buffer[k++] = data[j++];
        for (i = first; i < one_after_last; i++)
        data[i] = buffer[i];
free(buffer + first);
```

```
void insertMax(sum heap[], sum soma, int size)
{
    int i;
    for (i = size; i > 0 && heap[(i - 1) / 2].som < soma.som; i = (i - 1) / 2)
        heap[i] = heap[(i - 1) / 2];
        heap[i] = soma;
}

void insertMin(sum heap[], sum soma, int size)
{
    int i;
    for (i = size; i > 0 && heap[(i - 1) / 2].som > soma.som; i = (i - 1) / 2)
        heap[i] = heap[(i - 1) / 2];
        heap[i] = soma;
}
```

```
sum r = removeMin(minHeap, --nP);
r.ind1++;
               if (r.ind1 < (1 << nA))
                       int n = all_subset_sum_problems[i].n;
integer_t *p = all_subset_sum_problems[i].p;
double somaTempos = 0;
double tempoMaximo = 0;
int nB = n / 2;
int nD = n - nB;
int nA = nB / 2;
nB -= nA;
int nC = nD / 2;
 nD -= nC;
sum *sumsA = malloc((1 << nA) * sizeof(sum));
sum *sumsB = malloc((1 << nB) * sizeof(sum));
sum *sumsC = malloc((1 << nC) * sizeof(sum));
sum *sumsD = malloc((1 << nD) * sizeof(sum));</pre>
somas(nA, p, sumsA);
somas(nB, p + nA, sumsB);
somas(nC, p + nA + nB, sumsC);
somas(nD, p + nA + nB + nC, sumsD);
Merge(sumsA, 0, (1 << nA) - 1);
Merge(sumsB, 0, (1 << nB) - 1);
Merge(sumsC, 0, (1 << nC) - 1);
Merge(sumsD, 0, (1 << nD) - 1);
         integer_t desired = all_subset_sum_problems[i].sums[j];
double time = cpu_time();
sum minHeap[1 << nB];</pre>
```

sum s = {
 .som = sumsA[0].som + sumsB[a].som,
 .comb = sumsA[0].comb | (sumsB[a].comb << nA),
 .ind1 = 0,
 .ind2 = a);
insertMin(minHeap, s, nP++);</pre>

Código - MATLAB

```
%RECURSIVA
 valores = load("daniel2REC.txt");
 n1 = valores(1:end,1);
                               %primeira col
 tmax1 = valores(1:end,3);
                             %terceira col
 %RECURSIVA - otimizada
 valores = load("daniel2OTIM.txt");
 n = valores(1:end,1);
                              %primeira col
 tmed = valores(1:end,2);
                             %segunda col
                             %terceira col
 tmax = valores(1:end,3);
%% COMPARAR BRUTE FORCES
% RECURSIVAS
figure(5);
semilogy(n1,tmed1,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title('Comparação das Brute Forces')
hold on;
semilogy(n1,tmax1, '*-')
hold on;
semilogy(n,tmed,'+-');
hold on;
semilogy(n,tmax,'o-');
legend("tempoMédio", "tempoMáx", "tempoMédioOTIM", "tempoMáxOTIM");
xlim([10 36])
grid on;
hold off:
```

%% BF OTIM -> 3 PCS

```
%DANIEL
valores = load("danielOTIM.txt");
n = valores(1:end,1);
                                %primeira col
tmax = valores(1:end,3);
                               %terceira col
valores = load("daniel20TIM.txt");
n1 = valores(1:end,1);
                                %primeira col
tmed1 = valores(1:end,2);
                                %segunda col
tmax1 = valores(1:end,3);
                                 %terceira col
valores = load("gui OTIM.txt");
n2 = valores(1:end,1);
                                %primeira col
tmed2 = valores(1:end,2);
                                %segunda col
semilogy(n,tmed,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title('Brute Force Otimizada (Comparação 3 PCs)')
hold on;
semilogy(n,tmax, '*-')
hold on;
semilogy(n1,tmed1,'.-');
hold on;
semilogy(n1,tmax1, '*-')
hold on;
semilogy(n2,tmed2,'.-');
hold on;
semilogy(n2,tmax2, '*-')
legend("tempoMédioPC1", "tempoMáximoPC1", "tempoMédioPC2", "tempoMáximoPC2", "tempoMédioPC3", "tempoMédioPC3");
xlim([10 36])
grid on;
hold off;
```

```
%% BF REC -> 3 PCS
%DANIEL
 valores = load("danielREC.txt");
 n = valores(1:end,1);
                        %primeira col
 tmed = valores(1:end,2);
                        %segunda col
 valores = load("daniel2REC.txt");
 n1 = valores(1:end,1);
                       %primeira col
                      %segunda col
 tmed1 = valores(1:end,2);
                       %terceira col
 tmax1 = valores(1:end,3);
 valores = load("gui_REC.txt");
 %segunda col
 tmed2 = valores(1:end,2);
 tmax2 = valores(1:end,3);
                       %terceira col
%
semilogy(n,tmed,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title('Brute Force (Comparação 3 PCs)')
hold on;
semilogy(n,tmax, '*-')
```

hold on;

hold on;

hold on;

hold on;

hold on;

xlim([10 36])
grid on;
hold off;

semilogy(n1,tmed1,'.-');

semilogy(n1,tmax1, '*-')

semilogy(n2,tmed2,'.-');

semilogy(n2,tmax2, '*-')

legend("tempoMédioPC1", "tempoMáximoPC1", ...
 "tempoMédioPC2", "tempoMáximoPC2", ...
 "tempoMédioPC3", "tempoMáximoPC3");

```
%% COMPARAR AS RECURSIVAS - 3 pcs
clear;
clc;
close all;
%PC 1
valores = load("danielOTIM.txt");
nOTIM1 = valores(1:end,1);
                                 %primeira col
tmedOTIM1 = valores(1:end,2);
                                 %segunda col
tmaxOTIM1 = valores(1:end,3);
                                 %terceira col
%PC 2
valores = load("daniel2OTIM.txt");
nOTIM2 = valores(1:end,1);
                                 %primeira col
tmedOTIM2 = valores(1:end,2);
                                 %segunda col
tmaxOTIM2 = valores(1:end,3);
                                 %terceira col
valores = load("gui_OTIM.txt");
nOTIM3 = valores(1:end,1);
                                 %primeira col
tmedOTIM3 = valores(1:end,2);
                                 %segunda col
tmaxOTIM3 = valores(1:end,3);
                                 %terceira col
```

```
%pc1
valores = load("danielREC.txt");
                      %primeira col
n = valores(1:end,1);
tmed = valores(1:end,2);
                      %segunda col
tmax = valores(1:end,3);
                      %terceira col
%pc2
valores = load("daniel2REC.txt");
                   %primeira col
n1 = valores(1:end,1);
tmed1 = valores(1:end,2);
                      %segunda col
%рс3
valores = load("gui_REC.txt");
n2 = valores(1:end,1);
                      %primeira col
tmed2 = valores(1:end,2);
                      %segunda col
```

```
semilogy(n,tmed,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title('Brute Forces (Comparação 3 PCs)')
hold on;
semilogy(n,tmax, '*-')
hold on;
%pc2
semilogy(n1,tmed1,'.-');
hold on;
semilogy(n1,tmax1, '*-')
hold on;
%рс3
semilogy(n2,tmed2,'.-');
hold on;
semilogy(n2,tmax2, '*-')
hold on;
%pc1 OTIM
semilogy(nOTIM1,tmedOTIM1,'.-');
hold on;
semilogy(nOTIM1,tmaxOTIM1, '*-')
hold on;
%pc2 OTIM
semilogy(nOTIM2,tmedOTIM2,'.-');
hold on;
semilogy(nOTIM2,tmaxOTIM2, '*-')
hold on;
%pc3 OTIM
semilogy(nOTIM3,tmedOTIM3,'.-');
```

```
semilogy(nOTIM3,tmaxOTIM3, '*-')
hold on;
legend("tempoMédioPC1", "tempoMáximoPC1", ...
    "tempoMédioPC2", "tempoMáximoPC2", ...
    "tempoMédioPC3", "tempoMáximoPC3", ...
    "tempoMédioPC1OTIM", "tempoMáximoPC1OTIM", ...
    "tempoMédioPC2OTIM", "tempoMáximoPC2OTIM", ...
    "tempoMédioPC3OTIM", "tempoMáximoPC3OTIM");
xlim([10 36])
grid on;
hold off;
```

```
%% 3º e 4º algor
%horowitz
valores = load("danielHORO.txt");
n1 = valores(1:end,1);
                         %primeira col
tmed1 = valores(1:end,2);
                         %segunda col
tmax1 = valores(1:end,3);
                         %terceira col
%schroalgçaslçglçasçg
valores = load("danielSCH.txt");
n2 = valores(1:end,1);
                         %primeira col
tmed2 = valores(1:end,2);
                         %segunda col
```

```
% 3 e 4
figure(5);
semilogy(n1,tmed1,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title('Comparação 'Horowitz and Sahni' e 'Schroeppel and Shamir' (PC1)')
hold on;
semilogy(n1,tmax1, '*-')
hold on;
semilogy(n2,tmed2,'+-');
hold on;
semilogy(n2,tmax2,'o-');
legend("tempoMédioHORO", "tempoMáxHORO", "tempoMédioSCHR", "tempoMáxSCHR");
xlim([10 65])
grid on;
hold off;
```

```
%% COMPARAR
                            3 PCS
clear:
clc;
close all;
%horowitz
valores = load("danielHORO.txt");
nHORO1 = valores(1:end,1);
                                    %primeira col
tmedHORO1 = valores(1:end,2);
                                    %segunda col
tmaxHORO1 = valores(1:end,3);
                                    %terceira col
valores = load("daniel2HORO.txt");
nHORO2 = valores(1:end,1);
                                    %primeira col
tmedHORO2 = valores(1:end,2);
                                    %segunda col
tmaxHORO2 = valores(1:end,3);
                                    %terceira col
valores = load("guiHORO.txt");
nHORO3 = valores(1:end,1);
                                    %primeira col
tmedHORO3 = valores(1:end,2);
                                    %segunda col
                                    %terceira col
tmaxHORO3 = valores(1:end,3);
%schroppel
valores = load("danielSCH.txt");
nSCH1 = valores(1:end,1);
                               %primeira col
tmedSCH1 = valores(1:end,2);
                               %segunda col
tmaxSCH1 = valores(1:end,3);
                               %terceira col
valores = load("daniel2SCH.txt");
nSCH2 = valores(1:end,1);
                               %primeira col
tmedSCH2 = valores(1:end,2);
                               %segunda col
                               %terceira col
tmaxSCH2 = valores(1:end,3);
valores = load("guiSCH.txt");
nSCH3 = valores(1:end,1);
                               %primeira col
tmedSCH3 = valores(1:end,2);
                               %segunda col
tmaxSCH3 = valores(1:end,3);
                               %terceira col
```

```
% horo 1
semilogy(nHORO1,tmedHORO1,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title("'Horowitz and Sahni' e 'Schroeppel and Shamir' (Comparação 3 PCs)")
hold on;
semilogy(nHORO1,tmaxHORO1,'*-');
hold on;
% horo 2
semilogy(nHORO2,tmedHORO2,'.-');
hold on;
semilogy(nHORO2,tmaxHORO2,'*-');
hold on;
%horo 3
semilogy(nHORO3,tmedHORO3,'.-');
hold on;
semilogy(nHORO3,tmaxHORO3,'*-');
hold on;
%SCH 1
semilogy(nSCH1,tmedSCH1,'.-');
hold on;
semilogy(nSCH1,tmaxSCH1,'*-');
hold on;
```

```
93
            %SCH 2
94
            semilogy(nSCH2,tmedSCH2,'.-');
35
            hold on;
            semilogy(nSCH2,tmaxSCH2,'*-');
96
37
            hold on;
86
            %SCH 3
99
10
            semilogy(nSCH3,tmedSCH3,'.-');
            hold on;
11
            semilogy(nSCH3,tmaxSCH3,'*-');
12
13
            hold on;
14
            legend("tempoMédioPC1-HORO", "tempoMáximoPC1-HORO", ...
15
16
                 "tempoMédioPC2-HORO", "tempoMáximoPC2-HORO", ...
                 "tempoMédioPC3-HORO", "tempoMáximoPC3-HORO", ...
17
                 "tempoMédioPC1-SCH", "tempoMáximoPC1-SCH", ...
"tempoMédioPC2-SCH", "tempoMáximoPC2-SCH,", ...
"tempoMédioPC3-SCH", "tempoMáximoPC3-SCH");
18
19
20
21
            xlim([10 65])
22
            grid on;
23
            hold off;
24
25
```

```
%%
clear;
clc
close all;
%PC 1
valores = load("danielOTIM.txt");
nOTIM1 = valores(1:end,1);
                                  %primeira col
tmedOTIM1 = valores(1:end,2);
                                  %segunda col
tmaxOTIM1 = valores(1:end,3);
                                  %terceira col
%PC 2
valores = load("daniel20TIM.txt");
nOTIM2 = valores(1:end,1);
                                  %primeira col
tmedOTIM2 = valores(1:end,2);
                                  %segunda col
                                  %terceira col
tmaxOTIM2 = valores(1:end,3);
```

```
valores = load("gui OTIM.txt");
nOTIM3 = valores(1:end,1);
                                 %primeira col
tmedOTIM3 = valores(1:end,2);
                                 %segunda col
tmaxOTIM3 = valores(1:end,3);
                                 %terceira col
%normais
%pc1
valores = load("danielREC.txt");
n = valores(1:end,1);
                            %primeira col
tmed = valores(1:end,2);
                            %segunda col
tmax = valores(1:end,3);
                            %terceira col
%pc2
valores = load("daniel2REC.txt");
n1 = valores(1:end,1);
                             %primeira col
tmed1 = valores(1:end,2);
                             %segunda col
tmax1 = valores(1:end,3);
                             %terceira col
%рс3
valores = load("gui REC.txt");
                             %primeira col
n2 = valores(1:end,1);
tmed2 = valores(1:end,2);
                             %segunda col
tmax2 = valores(1:end,3);
                             %terceira col
```

```
%horowitz
valores = load("danielHORO.txt");
nHORO1 = valores(1:end,1);
                                 %primeira col
tmedHORO1 = valores(1:end,2);
                                 %segunda col
                                 %terceira col
tmaxHORO1 = valores(1:end,3);
valores = load("daniel2HORO.txt");
nHORO2 = valores(1:end,1);
                                 %primeira col
tmedHORO2 = valores(1:end,2);
                                 %segunda col
                                 %terceira col
tmaxHORO2 = valores(1:end,3);
valores = load("guiHORO.txt");
nHORO3 = valores(1:end,1);
                                 %primeira col
tmedHORO3 = valores(1:end,2);
                                 %segunda col
tmaxHORO3 = valores(1:end,3);
                                 %terceira col
%schroppel
valores = load("danielSCH.txt");
nSCH1 = valores(1:end,1);
                                  %primeira col
tmedSCH1 = valores(1:end,2);
                                  %segunda col
                                  %terceira col
tmaxSCH1 = valores(1:end,3);
valores = load("daniel2SCH.txt");
nSCH2 = valores(1:end,1);
                                  %primeira col
tmedSCH2 = valores(1:end,2);
                                  %segunda col
                                  %terceira col
tmaxSCH2 = valores(1:end,3);
valores = load("guiSCH.txt");
nSCH3 = valores(1:end,1);
                                  %primeira col
tmedSCH3 = valores(1:end,2);
                                  %segunda col
tmaxSCH3 = valores(1:end,3);
                                  %terceira col
```

```
%
semilogy(n,tmed,'.-');
ylabel("Tempo(s)");
xlabel("Variação de n")
title('Comparação Total - 3 PCs')
hold on;
semilogy(n,tmax, '*-')
hold on;
%pc2
semilogy(n1,tmed1,'.-');
hold on;
semilogy(n1,tmax1, '*-')
hold on;
%рс3
semilogy(n2,tmed2,'.-');
hold on;
semilogy(n2,tmax2, '*-')
hold on;
%pc1 OTIM
semilogy(nOTIM1, tmedOTIM1, '.-');
hold on;
semilogy(nOTIM1,tmaxOTIM1, '*-')
hold on;
%pc2 OTIM
semilogy(nOTIM2,tmedOTIM2,'.-');
hold on;
semilogy(nOTIM2,tmaxOTIM2, '*-')
hold on;
```

```
%pc3 OTIM
semilogy(nOTIM3,tmedOTIM3,'.-');
hold on;
semilogy(nOTIM3,tmaxOTIM3, '*-')
hold on;
% horo e 4
%HORO1
semilogy(nHORO1,tmedHORO1,'.-');
hold on;
semilogy(nHORO1,tmaxHORO1,'*-');
hold on;
% horo 2
semilogy(nHORO2, tmedHORO2, '.-');
hold on;
semilogy(nHORO2,tmaxHORO2,'*-');
hold on;
%horo 3
semilogy(nHORO3,tmedHORO3,'.-');
hold on;
semilogy(nHORO3,tmaxHORO3,'*-');
hold on;
%SCH 1
semilogy(nSCH1,tmedSCH1,'.-');
hold on;
semilogy(nSCH1,tmaxSCH1,'*-');
hold on;
%SCH 2
semilogy(nSCH2,tmedSCH2,'.-');
hold on;
semilogy(nSCH2,tmaxSCH2,'*-');
hold on;
%SCH 3
semilogy(nSCH3,tmedSCH3,'.-');
hold on;
semilogy(nSCH3,tmaxSCH3,'*-');
hold on;
```

```
legend("tempoMédioPC1", "tempoMáximoPC1", ...
    "tempoMédioPC2", "tempoMáximoPC2", ...
    "tempoMédioPC3", "tempoMáximoPC3", ...
    "tempoMédioPC1OTIM", "tempoMáximoPC1OTIM", ...
    "tempoMédioPC2OTIM", "tempoMáximoPC2OTIM", ...
    "tempoMédioPC3OTIM", "tempoMáximoPC3OTIM", ...
    "tempoMédioPC1-HORO", "tempoMáximoPC1-HORO", ...
    "tempoMédioPC2-HORO", "tempoMáximoPC2-HORO", ...
    "tempoMédioPC3-HORO", "tempoMáximoPC3-HORO", ...
    "tempoMédioPC1-SCH", "tempoMáximoPC1-SCH", ...
    "tempoMédioPC2-SCH", "tempoMáximoPC2-SCH,", ...
    "tempoMédioPC3-SCH", "tempoMáximoPC3-SCH");
xlim([10 65])
grid on;
hold off;
```