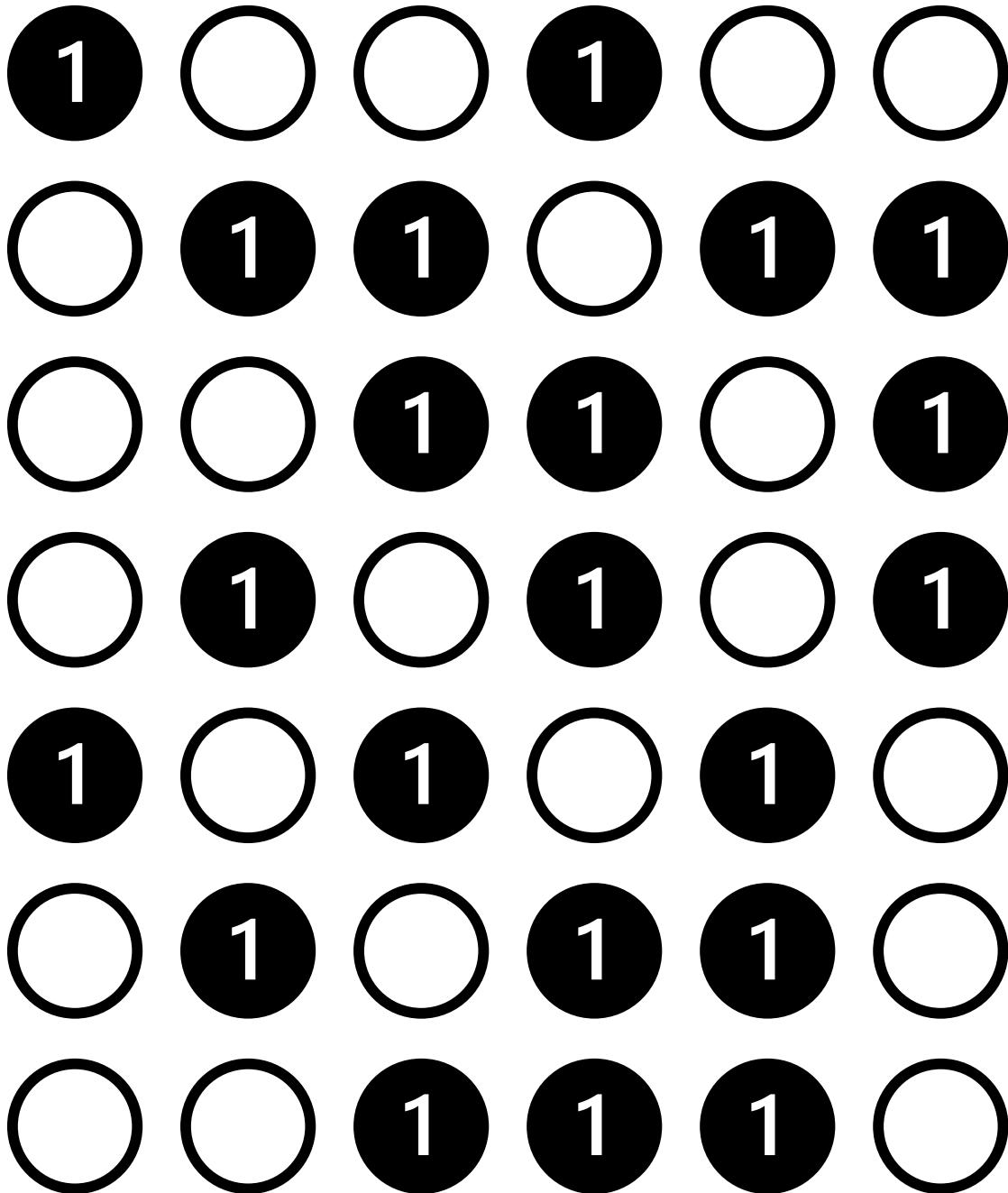


Aveiro, 9 de janeiro 2021



The Merkle-Hellman Cryptosystem

Mariana Andrade – 103823 – 50%

Vicente Barros – 97877 – 50%

Índice

Introdução	3
Contextualização do Problema.....	4
Brute Force.....	5
Clever Brute Force.....	6
Horowitz and Sahni Technique.....	7
Schroepel and Shamir Technique	8
Resultados Obtidos	9
Otimizações.....	9
Gráficos.....	9
Conclusão.....	11
Referências.....	12
Anexos	13
Código C.....	13
Código Matlab	19
Masks	20

Introdução

A criptografia é usada na comunicação de dados para proteger mensagens que circulam em canais de comunicação pouco seguros. Só na década de 70, com o aparecimento dos sistemas criptográficos de chave pública ou assimétrica, veio-se resolver o problema do transporte seguro de chaves.

O objetivo deste trabalho é a implementação e estudo de diversos algoritmos de decifragem do sistema criptográfico de Merkle-Hellman.

O problema proposto consiste na identificação de um subconjunto de um dado conjunto de números fornecido a priori, onde a soma dos elementos desse subconjunto corresponde à solução pretendida. O resultado final é apresentado na forma de uma *mask* onde o índice dos bits a 1 indica a posição no conjunto fornecido dos valores pertencentes ao subconjunto.

Para a resolução do problema foram implementados vários algoritmos de modo a mostrar as vantagens e desvantagens de cada um, onde os resultados obtidos vão ser descritos neste relatório.

Contextualização do Problema

Como referido anteriormente, o problema proposto (*subset sum problem*) consiste num conjunto de n inteiros positivos $\mathbf{P} = (p_0, p_1, \dots, p_{n-1})$ e ainda um inteiro positivo x . O objetivo do problema é identificar um subconjunto único $\mathbf{S} \subset \mathbf{P}$ onde:

$$x = \sum_{i=0}^{n-1} S_i$$

De modo a apresentar o resultado de uma forma clara, este vai ser representado na forma de uma *mask* $\mathbf{M} = (m_0, m_1, \dots, m_{n-1})$ onde $m_i \in \{0,1\}$ tal que:

$$x = \sum_{i=0}^{n-1} p_i m_i$$

O exemplo a seguir demonstra uma solução do problema.

$$\mathbf{P} = (234, 429, 769, 835, 858, 874, 998, 1200, 1592, 1655)$$

$$x = 5963$$

$$\mathbf{S} = (429, 769, 835, 858, 874, 998, 1200)$$

$$\mathbf{M} = (0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$$

Para alcançar as soluções, foram implementados quatro algoritmos: *Bruteforce*, *Clever Bruteforce*, *Horowitz e Sahni*, *Schroeppel e Shamir*, que vão ser explicados a seguir.

Brute Force

O método **Brute Force**, consiste numa implementação recursiva, onde são calculadas todas as combinações possíveis de *masks* até que **M** seja encontrado.

Assim, é passado como parâmetros de entrada o vetor **P** e o seu tamanho **n**, o nível de recursividade **level**, inicialmente a 0, a soma obtida até ao momento **partial_sum**, a soma pretendida **desired_sum** e a *mask* a ser testada **mask**.

A função começa por avaliar os casos de término, quando **level** é maior que **n**, significa que a solução não foi encontrada e, se **partial_sum** é igual **desired_sum**, o que significa que **x** foi encontrado.

O comportamento recursivo da função pode ser representado através de uma árvore onde cada nó representa uma **partial_sum**. Cada nó pai vai ter dois nós filho, onde **M_{level}** vai estar a 0 ou a 1 respetivamente, construindo assim todas as **M** possíveis. Ao verificar todas as hipóteses possíveis, este método vai ter $O(2^n)$ de execução para **M_n**.

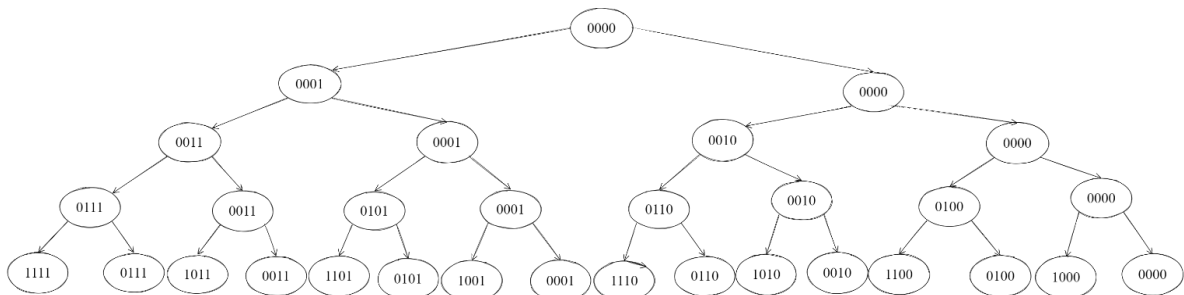


Figura 1- Árvore para n=4

Clever Brute Force

O método *Clever Brute Force*, tal como o nome indica, é uma versão do algoritmo explicado anteriormente, mas com otimizações que removem logo casos improváveis.

São passados como parâmetros os mesmos do método anterior e um vetor *sums* onde

$$Sums_1 = P_1 \text{ e } Sums_i = \sum_{j=2}^n Sums_{j-1} + P_j$$

Este método é mais eficiente que o anterior porque é efetuado o *pruning* de certos nós da árvore que nunca iriam resultar em *S*. É sabido do problema que $\forall p \in P, p_i < p_{i+1}, i \in N$ então, se *partial_sum* + *Sums_{level}* < *x* a *mask* que está a ser testada já não candidata a solução. Sendo assim, ao invés de testar de forma crescente as máscaras, começando com *P₀* começa-se a testar para *P_{n-1}* e de forma decrescente para eliminar mais rapidamente *masks*.

No entanto, este método apesar de ser mais eficiente, continua a ter de complexidade de execução $\mathcal{O}(2^n)$, visto que para o pior dos casos vai ter de testar todas as combinações possíveis.

Horowitz and Sahni Technique

O método *meet-in-the-middle*, idealizado por *E. Horowitz* e *S. Sahni* e tem como intento subdividir o problema. P é dividido em dois subconjuntos de tamanhos aproximadamente iguais, A e B e são geradas e guardadas em dois vetores todas as somas possíveis de cada subconjunto, $sumsA$ e $sumsB$ com tamanho aproximadamente $2^{n/2}$. Os vetores de somas são ordenados com recurso ao algoritmo *quicksort* por ordem crescente.

Sabendo que se $sumsA_i + sumsB_j = x$ então a solução foi encontrada. Para isto acontecer os dois vetores são percorridos por ordem crescente e decrescente, respetivamente e, caso $sumsA_i + sumsB_j < x$, i é incrementado e se $sumsA_i + sumsB_j > x$, j é decrementado. Caso $i > n_{sumsA}$ ou $j < 0$, a solução não foi encontrada.

Este método, reduz drasticamente a complexidade comparativamente aos métodos apresentados anteriormente tendo $\mathcal{O}(n2^{n/2})$ na execução, permitindo calcular soluções para n 's maiores. Contudo, ao calcular $sumsA$ e $sumsB$ há um grande dispêndio de memória.

¹ Ao correr o ficheiro *subset_sum_problem.c* o cálculo de $sumsA$ e $sumsB$ são efetuados antes de executar o algoritmo, visto que, para cada conjunto de problemas de tamanho igual, P é sempre o mesmo.

Schroeppele and Shamir Technique

O método de *Schroeppele* e *Shamir* surge com o objetivo de otimizar o método anterior ao reduzir a necessidade de bastante memória. Para isso ao invés de dividir P em 2, divide em 4 subconjuntos de tamanhos aproximadamente iguais, são gerados os vetores de somas *sumsA*, *sumsB*, *sumsC* e *sumsD* e estes são ordenados recorrendo outra vez ao algoritmo *quicksort*.

Os vetores *sumsA* e *sumsB* são usados para popular a *minHeap*, onde a raiz é a menor soma possível e *sumsC* e *sumsD* são usados para popular a *maxHeap*, onde a raiz é a maior soma possível. As *heaps* são usadas para gerar as somas entre os pares de subconjuntos *on the fly* para evitar o enorme consumo de memória ao calcular a soma quando essa é necessária.

Seguindo o método anterior, verifica se a soma das raízes das heaps é a soma pretendida. Caso a *partial_sum* seja maior que *desired_sum* a raiz da *maxHeap* é eliminada e substituída pelo próximo elemento e, se *partial_sum* seja menor *desired_sum* a raiz da *minHeap* é eliminada e substituída pelo próximo elemento.

Este método apresenta complexidade $\mathcal{O}\left(\frac{n}{4} 2^{\frac{n}{2}}\right)$, na execução e $\mathcal{O}\left(2^{\frac{n}{4}}\right)$ de memória, conseguindo assim corrigir o problema de memória do algoritmo anterior, conseguindo assim quebrar a barreira dos 64 bits.

Resultados Obtidos

Otimizações

Ao longo do desenvolvimento dos métodos implementados, foram feitas otimizações de código que melhoraram a performance de cada um. É de se destacar a conversão de ciclos em funções recursivas para o cálculo das somas, o uso de apontadores na divisão de P nos dois últimos métodos para evitar alocação de memória desnecessária e ainda a conversão da maioria das operações para operações *bitwise*.

Gráficos

Em cada um dos gráficos apresentados a seguir vai ser analisada a performance de cada um dos algoritmos consoante o N .

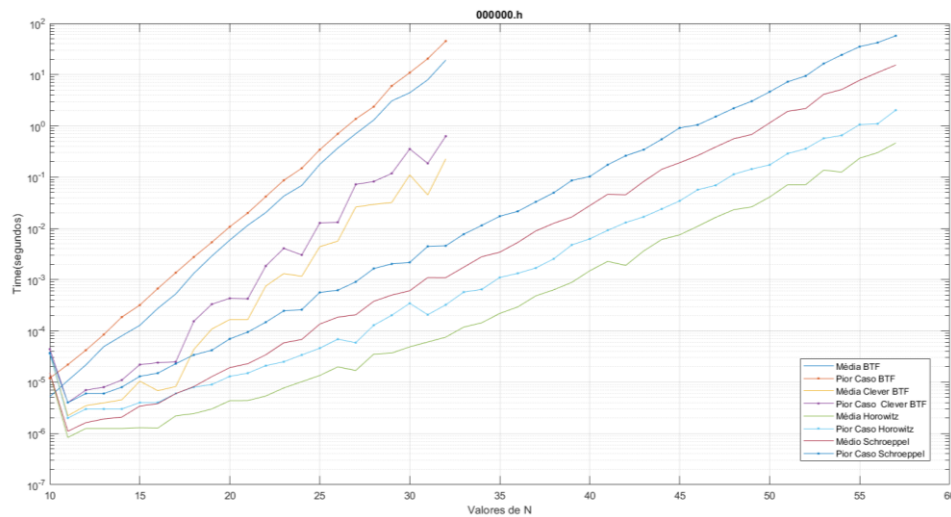


Figura 2- Gráfico do Tempo em função de N de 000000.h

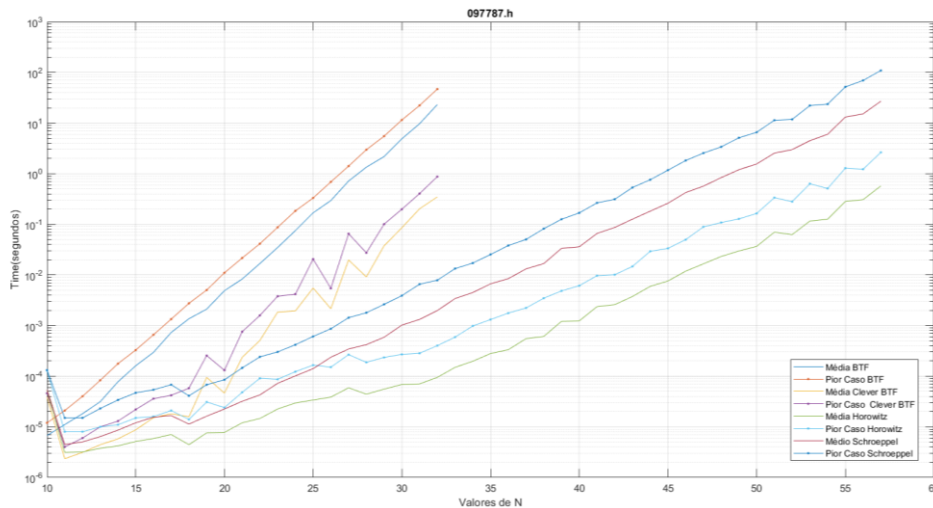


Figura 3 - Gráfico do Tempo em função de N de 097787.h

The Merkle-Hellman Cryptosystem

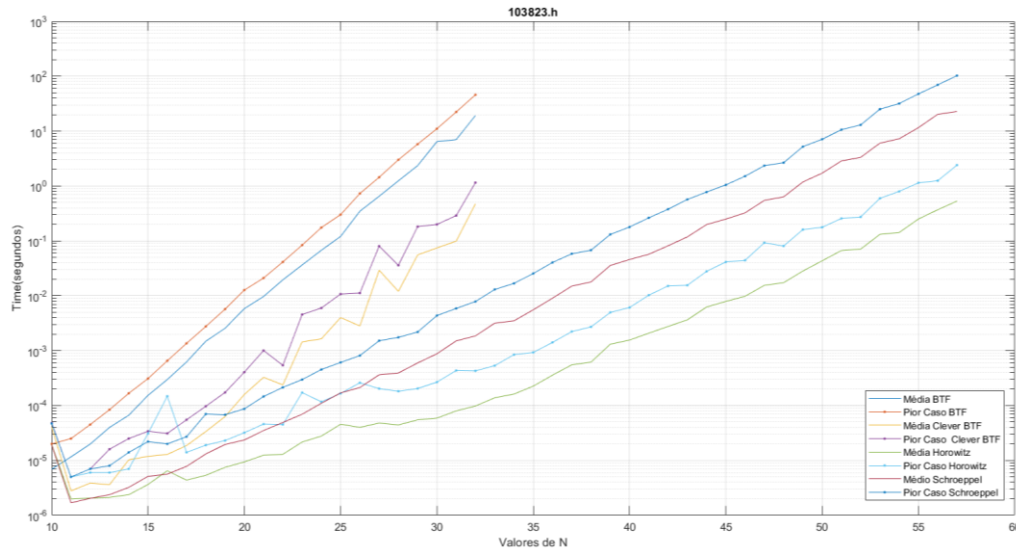


Figura 4- Gráfico do Tempo em função de N de 103823.h

Pode-se perceber facilmente que os algoritmos tiveram comportamentos semelhantes em todos os ficheiros fornecidos (000000.h, 097787.h e 103823.h), onde se destaca a fraca performance do *Brute Force* com uma diferença acentuada para o *Clever Brute Force*, este que apesar de apresentar melhorias à sua versão não otimizada, continua a ter um crescimento abrupto.

O método *Horowitz e Sahni* para n 's relativamente pequenos tem um comportamento inferior aos *Brute Forces*, mas à medida que n vai aumentando, é facilmente perceptível que consegue superar os métodos anteriores conseguindo alcançar valores de n muito superiores.

O método *Schroepel e Shamir*, tem um comportamento semelhante ao *Horowitz e Sahni* para n 's pequenos, consegue ter uma eficiência muito maior, devido ao facto de não ter de calcular conjuntos de somas tão grandes, nem de as ter de guardar em memória durante toda a sua execução.

Todos os valores usados neste relatório foram obtidos sempre com a mesma máquina com as seguintes características: Intel(R) Core (TM) i7-9750H CPU @ 2.60GHz 2.59 GHz; 16,0 GB RAM; Ubuntu 20.04.3 LTS e todos os valores usados para a construção dos gráficos foi incluído o cálculo das somas.

Conclusão

Com este trabalho, foi possível perceber o quão importante é a procura de várias soluções para o mesmo problema, para perceber as vantagens e desvantagens de cada um deles. Serviu também para aprender mais sobre as técnicas de otimização de código em C e para compreender a necessidade de gestão da memória que o programa precisa para correr.

Referências

Estruturas de dados e Algoritmos em C, António Adrego da Rocha, 3ª edição, FCA. Retrieved January 8, 2022

New generic algorithms for hard knapsacks. (n.d.). Retrieved January 8, 2022, from <https://eprint.iacr.org/2010/189.pdf>.

Subset sum problem - Wikipedia. (n.d.). Retrieved January 8, 2022, from https://en.wikipedia.org/wiki/Subset_sum_problem.

Merkle–Hellman knapsack cryptosystem - Wikipedia. (n.d.). Retrieved January 8, 2022, from https://en.wikipedia.org/wiki/Merkle%E2%80%93Hellman_knapsack_cryptosystem.

Meet in the middle - GeeksforGeeks. (n.d.). Retrieved January 8, 2022, from <https://www.geeksforgeeks.org/meet-in-the-middle>.

Anexos

Nesta secção está disponibilizado o código C que foi desenvolvido para as várias soluções apresentadas neste relatório e ainda o código Matlab utilizado para processar os resultados obtidos.

Código C

```
int bruteforce_iterativo(int n, integer_t p[n], integer_t desired_sum, integer_t * b) {
    for (int mask = 0; mask < 1 << n; mask++) {
        integer_t partial_sum = 0;
        for (int bit = 0; bit < n; bit++) {
            if (mask & (1 << bit))
                partial_sum += p[bit];
        }
        if (partial_sum == desired_sum) {
            * b = mask;
            return 1;
        }
    }
    return 0;
}

int bruteforce_rekursivo(int n, integer_t p[n], int level, integer_t partial_sum, integer_t desired_sum, integer_t
mask, integer_t * b) {
    if (level > n) {
        return 0;
    }
    if (partial_sum == desired_sum) {
        * b = mask;
        return 1;
    }

    if (bruteforce_rekursivo(n, p, level + 1, partial_sum + p[level], desired_sum, (mask | (1 << level)), b)) {
        return 1;
    } else {
        return bruteforce_rekursivo(n, p, level + 1, partial_sum, desired_sum, mask, b);
    }
}

int bruteforce_rekursivo_otimizado(int n, integer_t p[n], int level, integer_t partial_sum, integer_t desired_sum, integer_t mask,
integer_t * b, integer_t * sums) {
    if (partial_sum == desired_sum) {
        * b = mask;
        return 1;
    }

    if (level < 0 || partial_sum > desired_sum || partial_sum + sums[level] < desired_sum) {
        return 0;
    }

    if (bruteforce_rekursivo_otimizado(n, p, level - 1, partial_sum + p[level], desired_sum, (mask | (1 << (level))), b, sums)) {
        return 1;
    } else {
        return bruteforce_rekursivo_otimizado(n, p, level - 1, partial_sum, desired_sum, mask, b, sums);
    }
}
```

The Merkle-Hellman Cryptosystem

```
typedef struct {
    integer_t mask;
    integer_t sum;
}
mask_data_t;

void swap(mask_data_t * a, mask_data_t * b) {
    mask_data_t t = * a;
    * a = * b;
    * b = t;
}

int partition(mask_data_t arr[], int low, int high) {
    mask_data_t pivot = arr[high]; // pivot
    int i = (low - 1); // Index of smaller element and indicates the right position of pivot found so far

    for (int j = low; j ≤ high - 1; j++) {
        // If current element is smaller than the pivot
        if (arr[j].sum < pivot.sum) {
            i++; // increment index of smaller element
            swap( & arr[i], & arr[j]);
        }
    }
    swap( & arr[i + 1], & arr[high]);
    return (i + 1);
}

void quicksort(mask_data_t arr[], int low, int high) {
    if (low < high) {
        /* pi is partitioning index, arr[p] is now
        at right place */
        int pi = partition(arr, low, high);
        // Separately sort elements before
        // partition and after partition
        quicksort(arr, low, pi - 1);
        quicksort(arr, pi + 1, high);
    }
}

void sums_generator(int n, integer_t p[n], mask_data_t result[1 << n], int level, integer_t mask, integer_t subSum, int idx) {
    if (level == n) {
        result[idx].sum = subSum;
        result[idx].mask = mask;
        return;
    }
    sums_generator(n, p, result, level + 1, mask | (1 << level), subSum + p[level], 2*idx);
    sums_generator(n, p, result, level + 1, mask, subSum, 2*idx+1);
}

int horowitz_sahni(int n, integer_t p[], integer_t desired_sum, integer_t * b_result, mask_data_t *sumsA, mask_data_t *sumsB,
int nA, int nB) {
    int i = 0, j = (1 << nB) - 1;
    while (i < (1 << nA) && j ≥ 0) {
        if (sumsA[i].sum + sumsB[j].sum == desired_sum) {
            *b_result = sumsA[i].mask | (sumsB[j].mask << nA);
            return 1;
        } else if (sumsA[i].sum + sumsB[j].sum < desired_sum) {
            i++;
        } else {
            j--;
        }
    }
    return 0;
}

typedef struct {
    integer_t mask;
    integer_t sum;
    int i0;
    int i1;
} heapData_t;

void minheapInsert(heapData_t heap[], heapData_t element, int* heapSize)
{
    int i;
    for (i = *heapSize; i > 0 && heap[(i - 1) / 2].sum > element.sum; i = (i - 1) / 2)
    {
        heap[i] = heap[(i - 1) / 2];
    }
    heap[i] = element;
    (*heapSize)++;
}
```

The Merkle-Hellman Cryptosystem

```
heapData_t deleteMin(heapData_t heap[], int* heapSize)
{
    int i, son;
    heapData_t element = heap[0];

    (*heapSize)--;
    for (i = 0; i * 2 + 1 ≤ *heapSize; i = son) {
        son = 2 * i + 1;
        if (son < *heapSize && heap[son].sum > heap[son + 1].sum)
            son++;
        if (heap[son].sum < heap[*heapSize].sum)
            heap[i] = heap[son];
        else
            break;
    }

    heap[i] = heap[*heapSize];
    return element;
}

void maxheapInsert(heapData_t heap[], heapData_t element, int* heapSize)
{
    int i;
    for (i = *heapSize; i > 0 && heap[(i - 1) / 2].sum < element.sum; i = (i - 1) / 2) {
        heap[i] = heap[(i - 1) / 2];
    }
    heap[i] = element;
    (*heapSize)++;
}

heapData_t deletemax(heapData_t heap[], int* heapSize)
{
    int i, son;
    heapData_t element = heap[0];

    (*heapSize)--;
    for (i = 0; i * 2 + 1 ≤ *heapSize; i = son) {
        son = 2 * i + 1;
        if (son < *heapSize && heap[son].sum < heap[son + 1].sum)
            son++;
        if (heap[son].sum > heap[*heapSize].sum)
            heap[i] = heap[son];
        else
            break;
    }

    heap[i] = heap[*heapSize];
    return element;
}
```

The Merkle-Hellman Cryptosystem

```
int schroeppel_shamir (int n, integer_t p[], integer_t desired_sum, integer_t * b_result, mask_data_t *sumsA,mask_data_t *sumsB,
mask_data_t *sumsC, mask_data_t *sumsD,int nA, int nB, int nC, int nD) {
    heapData_t minHeap[1 << nB];
    heapData_t maxHeap[1 << nC];
    int nHMin = 0;
    int nHMax = 0;

    for (int i = 0; i < (1 << nB); i++) {
        heapData_t sum = {
            .mask = sumsA[0].mask | (sumsB[i].mask << nA),
            .sum = sumsA[0].sum + sumsB[i].sum,
            .i0 = 0,
            .i1 = i
        };
        minheapInsert(minHeap, sum, &nHMin);
    }

    for (int i = 0; i < (1 << nC); i++) {
        heapData_t sum = {
            .mask = sumsC[i].mask | (sumsD[(1 << nD) - 1].mask << nC),
            .sum = sumsC[i].sum + sumsD[(1 << nD) - 1].sum,
            .i0 = i,
            .i1 = (1 << nD) - 1
        };
        maxheapInsert(maxHeap,sum,&nHMax);
    }

    while (nHMin > 0 && nHMax > 0){
        integer_t partial_sum = maxHeap[0].sum + minHeap[0].sum;
        if (partial_sum == desired_sum) {
            *b_result = minHeap[0].mask | (maxHeap[0].mask << (nA+nB));
            return 1;
        } else if (partial_sum > desired_sum){
            heapData_t old_max = deletemax(maxHeap,&nHMax);
            old_max.i1--;

            if (old_max.i1 >= 0) {
                heapData_t new = {
                    .mask = sumsC[old_max.i0].mask | (sumsD[old_max.i1].mask << nC),
                    .sum = sumsC[old_max.i0].sum + sumsD[old_max.i1].sum,
                    .i0 = old_max.i0,
                    .i1 = old_max.i1
                };
                maxheapInsert(maxHeap,new,&nHMax);
            }
        } else {
            heapData_t old_min = deleteMin(minHeap, &nHMin);
            old_min.i0++;
            if (old_min.i0 < (1 << nA)) {
                heapData_t new = {
                    .mask = sumsA[old_min.i0].mask | (sumsB[old_min.i1].mask << nA),
                    .sum = sumsA[old_min.i0].sum + sumsB[old_min.i1].sum,
                    .i0 = old_min.i0,
                    .i1 = old_min.i1
                };
                minheapInsert(minHeap, new, &nHMin);
            }
        }
    }
    return 0;
}
```


The Merkle-Hellman Cryptosystem

```
int main(void) {
    fprintf(stderr, "Program configuration:\n");
    fprintf(stderr, "  min_n ..... %d\n", min_n);
    fprintf(stderr, "  max_n ..... %d\n", max_n);
    fprintf(stderr, "  n_sums ..... %d\n", n_sums);
    fprintf(stderr, "  n_problems .. %d\n", n_problems);
    fprintf(stderr, "  integer_t ... %d bits\n", 8 * (int) sizeof(integer_t));
    //
    // for each n
    //
    for (int i = 0; i < n_problems; i++) {
        int n = all_subset_sum_problems[i].n; // the value of n
        if (n > 42)
            continue; // skip large values of n
        integer_t * p = all_subset_sum_problems[i].p; // the weights
        //
        // for each sum
        //
        double start = cpu_time();
#ifdef BTF_RCR_OTM
        integer_t * sums = (integer_t *) malloc(n * sizeof(integer_t));

        sums[0] = p[0];
        for (int i=1; i<n; i++) {
            sums[i] = sums[i-1]+p[i];
        }
#endif

#ifdef HW_SN
        int nA = n / 2;
        int nB = n - nA;
        integer_t *a,*b;
        a = p;
        b = p + nA;
        mask_data_t * sumsA = malloc((1 << nA) * sizeof(mask_data_t));
        mask_data_t * sumsB = malloc((1 << nB) * sizeof(mask_data_t));

        sums_generator(nA, a, sumsA, 0, 0, 0, 0);
        quicksort(sumsA, 0, (1 << nA) - 1);

        sums_generator(nB, b, sumsB, 0, 0, 0, 0);
        quicksort(sumsB, 0, (1 << nB) - 1);
#endif

#ifdef MIM

        int nA = n / 4;
        int nB = n/2 - nA;
        int nC = nB;
        int nD = n - nA-nB-nC;

        integer_t * a = p;
        integer_t * b = p+nA;
        integer_t * c = p+nA+nB;
        integer_t * d = p+nA+nB+nC;
        mask_data_t * sumsA = malloc((1 << nA) * sizeof(mask_data_t));
        mask_data_t * sumsB = malloc((1 << nB) * sizeof(mask_data_t));
        mask_data_t * sumsC = malloc((1 << nC) * sizeof(mask_data_t));
        mask_data_t * sumsD = malloc((1 << nD) * sizeof(mask_data_t));

        //Para o Array A
        sums_generator(nA, a, sumsA, 0, 0, 0, 0);
        quicksort(sumsA, 0, (1 << nA) - 1);

        //Para o Array B
        sums_generator(nB, b, sumsB, 0, 0, 0, 0);
        quicksort(sumsB, 0, (1 << nB) - 1);

        //Para o Array C
        sums_generator(nC, c, sumsC, 0, 0, 0, 0);
        quicksort(sumsC, 0, (1 << nC) - 1);
        //Para o Array D
        sums_generator(nD, d, sumsD, 0, 0, 0, 0);
        quicksort(sumsD, 0, (1 << nD) - 1);
#endif
        double end = cpu_time();

        printf("%lf\n", end - start);
    }
}
```

The Merkle-Hellman Cryptosystem

```
for (int j = 0; j < n_sums; j++) {
    integer_t desired_sum = all_subset_sum_problems[i].sums[j]; // the desired sum
    integer_t b = 0; // array to record the solution
    double start = cpu_time();
    #ifdef BTF_ITR
        bruteforce_iterativo(n, p, desired_sum, &b);
    #endif

    #ifdef BTF_RCR_NOTM
        bruteforce_recurativo(n, p, 0, 0, desired_sum, 0, &b);
    #endif

    #ifdef BTF_RCR_OTM
        bruteforce_recurativo_otimizado(n, p, n - 1, 0, desired_sum, 0, &b, sums);
    #endif

    #ifdef HW_SN
        horowitz_sahni(n, p, desired_sum, &b, sumsA, sumsB, nA, nB);
    #endif

    #ifdef MIM
        schroeppeel_shamir(n, p, desired_sum, &b, sumsA, sumsB, sumsC, sumsD, nA, nB, nC, nD);
    #endif

    double end = cpu_time();

    for (int i = 0; i < n; i++) {
        printf("%s", b & 1 ? "1" : "0");
        b = b >> 1;
    }
    printf(" %lf\n", end - start);
}
#ifdef BTF_RCR_OTM
    free(sums);
#endif
#ifdef HW_SN
    free(sumsA);
    free(sumsB);
#endif
#ifdef MIM
    free(sumsA);
    free(sumsB);
    free(sumsC);
    free(sumsD);
#endif
return 0;
}
```

The Merkle-Hellman Cryptosystem

Código Matlab

```
function Grafico(namefile,x)
%vai buscar o calculo das somas feitas antes do algoritmo
% brute force para cada numero mecanografico (1,2,3)
% clever brute force para cada numero mecanografico (4,5,6)
% Horowitz para cada numero mecanografico (7,8,9)
% schroepel para cada numero mecanografico (10,11,12)
switch(x)
    case 1
        somas=load("000000\brute force_notz_somas_000000.txt");
    case 2
        somas=load("097787\brute force_notz_somas_097787.txt");
    case 3
        somas=load("103823\brute force_notz_somas_103823.txt");
    case 4
        somas=load("000000\brute force_otz_somas_000000.txt");
    case 5
        somas=load("097787\brute force_otz_somas_097787.txt");
    case 6
        somas=load("103823\brute force_otz_somas_103823.txt");
    case 7
        somas=load("000000\schroepel_somas_000000.txt");
    case 8
        somas=load("097787\schroepel_somas_097787.txt");
    case 9
        somas=load("103823\schroepel_somas_103823.txt");
    case 10
        somas=load("000000\schroepel_somas_000000.txt");
    case 11
        somas=load("097787\schroepel_somas_097787.txt");
    case 12
        somas=load("103823\schroepel_somas_103823.txt");
    case 13
        somas=load("097787\schroepel_somas_128_097787.txt");
end

T=load(namefile);%Valores do tempo para cada soma
T= T+somas';
[n,~]=size(T);
N=10:9+n;

ValorMaximoLinha = max(T'); %ValorMaximoLinha = max(data,[],2);
%ValorMinimoLinha= min(T'); %ValorMaximoLinha = min(data,[],2);
media = sum(T,2)/length(N); %media = sum(Q2')/length(N)

%grafico
semilogy(N,media)
hold on
semilogy(N,ValorMaximoLinha,"--");
hold on
%semilogy(N,ValorMinimoLinha,"--");
%hold on

end

clc
clear
close all

%000000
figure(1)
Grafico ("000000\brute force_notz_resultados_somas_000000_organizado.txt",1); %brute force para 64 bits
Grafico ("000000\brute force_otz_resultados_somas_000000_organizado.txt",4); %clever brute force para 64 bits
Grafico ("000000\horowitz_resultados_somas_000000_organizado.txt",7); %horowitz and sahni technique para 64 bits
Grafico ("000000\schroepel_resultados_somas_000000_organizado.txt",10); %schroepel and shamir technique para 64 bits

grid on;
title("000000.h")
legend( "Média BTF", "Pior Caso BTF", "Média Clever BTF", "Pior Caso Clever BTF", "Média Horowitz",
"Pior Caso Horowitz", "Médio Schroepel ", "Pior Caso Schroepel ");
xlabel("Valores de N");
ylabel("Time(segundos)");
hold off;

%097787
figure(2)
Grafico ("097787\brute force_notz_resultados_somas_097787_organizado.txt",2); %brute force para 64 bits
Grafico ("097787\brute force_otz_resultados_somas_097787_organizado.txt",5); %clever brute force para 64 bits
Grafico ("097787\horowitz_resultados_somas_097787_organizado.txt",8); %horowitz and sahni technique para 64 bits
Grafico ("097787\schroepel_resultados_somas_097787_organizado.txt",11); %schroepel and shamir technique para 64 bits
% Grafico ("097787\schroepel_128_resultados_somas_097787_organizado.txt",13); %schroepel and shamir technique(128)

grid on;
title("097787.h")
legend( "Média BTF", "Pior Caso BTF", "Média Clever BTF", "Pior Caso Clever BTF", "Média Horowitz",
"Pior Caso Horowitz", "Médio Schroepel ", "Pior Caso Schroepel ");
xlabel("Valores de N");
ylabel("Time(segundos)");
hold off;

%103823
figure(3)
Grafico ("103823\brute force_notz_resultados_somas_103823_organizado.txt",3); %brute force para 64 bits
Grafico ("103823\brute force_otz_resultados_somas_103823_organizado.txt",6); %clever brute force para 64 bits
Grafico ("103823\horowitz_resultados_somas_103823_organizado.txt",9); %horowitz and sahni technique para 64 bits
Grafico ("103823\schroepel_resultados_somas_103823_organizado.txt",12); %schroepel and shamir technique para 64 bits

grid on;
title("103823.h")
legend( "Média BTF", "Pior Caso BTF", "Média Clever BTF", "Pior Caso Clever BTF", "Média Horowitz",
"Pior Caso Horowitz", "Médio Schroepel ", "Pior Caso Schroepel ");
xlabel("Valores de N");
ylabel("Time(segundos)");
hold off;
```

The Merkle-Hellman Cryptosystem

Masks

Nesta secção estão dispostas as soluções obtidas para o problema proposto para cada um dos números mecanográficos.

	097787.h	103823.h
10	1100001110 0100010001 1000011000 0001101101 1100001011 1110111100 0000010111 1010111110 0011101010 0111001100 0101001000 1101000001 0111110110 0010001110 1100011101 0000101100 0011011100 0010100001 1111011100 000111011	0110101111 0101111111 1010101100 0010111111 0001010010 0010100110 0000011010 0001111101 1011010000 0010001010 0101111100 1100001110 1111111010 111000000 0010001110 0011010111 1011000101 1001101011 1101111000 111000111
11	0001101110 0110100110 0010010101 1010011101 1100001101 0001010110 0111001110 1000111000 1011101001 1110101000 0010011101 0100000111 1101000001 1001000100 0111100011 0111111111 1000100101 0110111000 1000010101 0100110010	11100100001 01010001000 1110111111 00001110001 10001011001 10010100100 10000111010 10111001100 00110100010 10001000110 10110011011 0100100011 01010111101 10010010110 0010110011 01110111000 01001001010 01100001110 0011101101 11110100110
12	101110010011 000101111100 111100011111 110000100100 001100101100 000100010100 000101101011 011010000000 010001110100 111000110110 111101101101 110101100011 111111011001 110000110010 100011101101 001111000111 001110010101 110101011101 100010111010 01011110111	011001001011 101001100000 000011011011 001100010010 100110111110 111001100100 011111000010 111110010001 000010111000 110000011111 101001111011 001101101010 001011110010 100101000110 101100010110 111101100100 100011101010 110101101110 000011010110 00101111111
13	1101000011100 1100101010111 1111101100111 0000110011011 0011010100010 1011000110001 1001101111011 1111100001010 1001101011111 0001100011101 1010010110100 0001000010110 1000111110110 1100100000111 1110111010000 0000010101111 1001011111111 1110010011010 111111110111 0111000110100	0111010010110 0110010110011 0111011000000 1001000001011 0101110000001 0000001100100 1000111001010 1011001001101 1000101010001 0010011111010 1011110010000 0101100100110 111110011010 0101000100111 1010011100011 1101111110100 0111111001010 1000001001000 0011010000110 0001110111110
14	10100111101010 00010001011100 11011011110111 00010100010101 00011011101011 10110101001000 1111111001111 01000010111001 11110100000000 0101111011111	00110110000101 10111010100100 10111011101110 100110100001001 00110010101111 10010110001010 00000011111010 01011100001101 10010111001011 11010001010101

The Merkle-Hellman Cryptosystem

	1110111111011 00111010110110 01001010101110 10110010111111 00010000111110 11011101111101 00001111110010 1111100100000 00100101001101 01001101111010	11110001101100 11001001011000 11011101110001 11111000010011 01001101100110 11000100100111 00100110111001 10001101100000 10100110110111 10011100010001
15	000111101100111 111101100011010 010101001010110 111010110100011 001001001111011 000111110001100 010010011110111 011010111111011 001010001100111 001100111100111 111001101001000 100001010001011 101100011001000 111011001011110 010110000011010 000100011100101 111011100101101 000111100001000 100000011001101 011110100111100	001111101000010 010011110001001 100010010101010 010111010010001 001111000100000 101010111100111 110000011010011 011011111000111 111111100010110 010101000000100 011010011100111 110010110010010 011000000110100 110111001010011 000111000010001 010011001001000 111101100110100 110000010001101 001000011100110 000101001100011
16	010100011010110 0000100110000101 0100110001111011 0011001001001010 0100001001010110 0100110001100101 1111001001100011 1011110111001101 1111010110110101 0111001111110111 0011101000001011 1100110100010110 1111100101110010 011001001010111 0110111010100010 1100010101101110 0000011001000110 1011000111011011 0101111011010010 1111010011000010	0110001100111110 10010010101111001 1110101001011001 1111010101001100 1110010010100001 0010000100001001 1100101100001101 0011010100011011 0010001110010100 1001110001010001 1111110111000001 1110001101110000 1010110111111010 0010001100001100 0110000010100101 0000101000001010 0100000110000001 0000100010100000 1000001101110000 0110100111010100
17	00100010100011110 10100100101110110 11101101100011101 11110001111011011 10101001110001001 00010010111001110 11101010001100010 00010100001000100 00010101001001111 01001111000111001 00111100100110000 01001001001111001 00011010001000011 01101001001001101 11110101010100011 01001011000011100 10011111111101111 00000011110101000 00111100100011101 0110000010110111	00000010011001110 00110001101011010 11010010010100010 10011011101010101 10101001000010111 01111111010000111 10100000101000111 00110110100100100 01111000000101110 11101010011000100 00011010110010000 10111101111100000 10011100010000100 10000111001011111 01101011111101110 11101111110011110 01101101111100111 00100111110101011 00010010111010011 01110000111001100
18	00000111111011011 001110001011111011 010001001101011010 001000101100011110 111101110001111000 000000111100101010 100001010101001101 001011001000110011 101011001101101011 100001101010011001 101011110010010010 100100010110001001 000101001111000111 011101010011010111 110011110101101111 011110001111000101 000100001110011010 001010100001101111 111100011110100101 111000011001001000	101110101001011100 010010011110110000 100001000001111010 011101111011111111 100000010000000011 001100000110100010 100110011111110110 001010111111010011 000010010101111111 111100110001101100 000010001011010000 000001111100110001 001101110011001110 000000110010011011 110101101000001010 000101000101111011 100000001010011111 110101001100110010 001101011111010001 010111100110000010
19	1000010010100101001 1111001101101011110 1000110111010000010 1000100011111000000 0110011011001010010 0111001100110110011 1010010111101010000 1010001001101100001 1100010001110010110 1111110101110100101 0011011010000110011 1100111111010101111 0111001000010010010 100111001101000011 100111001101000011	0110100110011101100 1001101001110100101 1001010100011110100 1010100010011001001 0001101010111111000 0101011000000010100 1001011010011010101 1011101000011001000 1011011011010011011 0010100010010011001 100101110010011110 1101011101001110110 0011111000010001111 1111011000011010111

The Merkle-Hellman Cryptosystem

	0100110001100001101 1001000101111011111 1001100100010001010 1000001111011011111 0001001010011111110 10011001111100001	1000101011010100000 0011010101100100101 0101100100100100001 00011010111000111 1010011100101110000 000100100111011001
20	10110000001101100011 1100111100111100110 10110101000010101011 01100100101000010000 0000110100110111010 0011001011010110111 1110111111010011101 0101111101110110001 1101000010000010011 0111011100010010011 00101011101101100111 0001001101110101101 1010111111011101110 0111110100010110101 10100000111010011000 011111010001001101 00101000101010100 0101010010110100000 1010010111011100101 1011101010100100010	00111000100111100011 11111110010001101110 01100000111110001100 10001111010101101101 01011110000111110011 1110000010100011010 001001101111011101 1000010010011101110 0011000010000000111 00100011011001100110 00011001111110100110 01101001100010000010 0110011110001001111 1001101001011110101 0011110010101011101 00011000101000001000 10001100000101000101 01010010010001010110 0000110000111101110 1111101001111000001
21	101000011101010111111 001001110100111110010 11100011110010010000 10101110000101110011 10100010111011100111 010100100110011110110 10111011111101100000 000010001100001110010 110010001100011010001 010100010000001000101 100101011100110101110 010101000110010111110 110010011001001101001 100111100001001011011 100010110101100110111 101000110110001011000 111100110010000101001 111001000101000001001 11001100100110111100 000001001110001101011	010111110100011001101 11101111111000110011 011000101000001111111 110010110111011010111 011101000111100101111 000111110001110000101 010101111000001110011 111000010010111000001 100010011100010010111 010110100011010111010 00011001011110101011 001000010000101110110 001000010000101110110 110000001001001110101 010011111101100111100 000110101001111101111 101010010000111010100 100110000100010100110 111111110010000100001 010100101011100001001 11100001111101010010
22	0110110111001110101111 1000011000101100001011 0110100101000001101101 0110011000011001111011 110101111100101000010 1001011111101101110011 1110110011011010110100 1011010010011101111110 101001100101111001111 1111100011011110001101 0100010011101101011101 0001010001110000101000 0011110001011010100111 1100010000101001100011 1111101001011101100101 1110001110111101110000 0100010100110110111000 0101010001111101011101 010000110001111110011 1011101111000111011001	0111011010000111100110 1001011000011111100011 1000000101111010010011 1111110010110010110001 1010001001010001011010 110010111111110101100 001001010111111111101 0001111111010111011101 0001000011110011001010 0001101010111011110110 0000111011010010011011 101111100101101101101 1000000100011001001110 1000100110011001110101 010111100001100101010 0101100111101000100100 0011100111011110101110 1101111000100001000011 111111001111101101001 1111001111010110001110
23	11110010111101100000011 110101010111011100110 10011110000011111111101 01010001010011101011010 00000010011000010111110 01100101111101101011110 01000001010111000000100 10001111011101000101100 11100101001010110101110 00110000010010111001010 10001001111110100010101 0101011001010111000110 11110110100110001010110 11011011101111010100001 00100110110011001101111 01000110010011111100001 11010110111011100100101 11101110100111001101001 1111111100000001100100 00000001011011011100010	01111110100110011110000 10110010110111001010110 01101000001010001000011 11111110000100101000010 10100100010110010110011 00001010100111101111101 000111010101110001010001 11101001100001011011110 01111110010111100011111 11010001110111010010010 00010011100111111010100 10110101110100001101101 10000101111000011100010 10011101011110011010100 0000110111110000110111 10101101010010111111100 01101010000110010011111 10111101000010010001111 10000111101010001101000 10011101000001000100101
24	110010010000011101001111 101100011000100000111110 110111100000010001110110 011010100011100011110000 000010001110111110111010 000110101010111001001000 010011100111101100100101 00010101111100000110111 010110011001011110010100 111111110111011000110010 01111000011101111000100 111001000101101111100110 101100001010000101100101 0110101101011110100100 010000000111001110011101 101011101010100110010011 101001000101110101011000 100010101101110100010001	010111110111100111011101 000010111010110100101000 10111111011101000001100 111010110100001011100100 111111011100001110010001 111001001110010000001011 10000010110110001101101 00110010111111010010001 110011001110111101101001 000111110010001000100110 111011010111100000100110 100101011100011011111110 011100100100001000100001 111000111000100010011001 100000001110111010010101 000100100100001011001000 10100001101111010011000 110001010000110011000101

The Merkle-Hellman Cryptosystem

	000110100001010101110101 111011111101010110011001	010110000011010110011111 100010000010010110011110
25	1000010000101111110111011 0001000111100001101001100 0111100110111100000010001 1001000011101100010010001 0011110001000010000110100 0001100000101110011001110 0010010011100000100001101 100000001111011111011111 1001001000011011100101010 1110100100010110111100011 1100011000110010000000001 0101000101000110100101101 0110000110011000010110101 1100101101101000011111111 0001011110110011101010101 1101000101000010100011101 111110011110001110100100 0010010110010101010010010 1011100001010000011000100 0010111110011010111110010	1010011110000110100100011 100111000110110001000011 110111101010011000000101 0111101010111111100000110 0010100111011011000111110 0101111100100001110100101 101100000110111011010101 1000011100011011110100010 100110001101111000100110 1000111100110011100010010 0100101101011010010111000 1111100000011001011000110 0110010111000011001000110 1111101001010000101110011 100111101010110011001010 110110101110101010111110 1011101000110110101000100 1010100001001001101011000 1110111000101100100000101 011010100101101000010011
26	110100111100100101110000010 1110111011011111000011011 00101110101111001110001000 11100100111000000000011110 0101000010101111111000011 00100110100110011001000100 0001011111011010111100001 0010011011010000011001111 1111111100100000001000110 11100011100110011011100011 0000011100110010101100001 11011010110110000000001110 11011001000000111000100110 11010011010000100100110000 0110000110100110110111100 01110011100000101011100110 0010101110101010010111001 10110001010101111101001010 0011111111110010101100011 10010001101100111010110101	01011010000011100100001101 10000001011110101001110001 00000100101001110001100111 10011000010001101101101011 11111010100100000000110001 00000111000011100001011011 1001001001110111011001011 00010001010011100110001100 10111110000110101000101000 00000010110111100000001111 10100011100010010110001010 00111110110011111001110110 11100010010101100000000001 00101101011101100111100111 1111010111101011111000111 10110110010110010111000100 10010010111110110110010100 00001101001011011000101001 00101101001101011000000100 11001001110101010011100111
27	101010100011010100100000100 000000101001010011001001011 100111111110101110100010000 10111011111110011000001011 100101110111010110011000011 10110001001110110111111100 10111010001001010101011001 001001011000010001001101100 000011010011011100100010100 100110111010011100101101100 010111110010000100100111010 110011101001100000000011010 1010011000010100010001010110 100010001100110010001000011 001100010111010000011101010 010000011101011001001001011 00101100000011001110111110 001011011110000101110010011 001111000100100111001110111 011101010010011001000101001	000011100010111100110100001 10101111010110001111111101 10001011000111011001110100 101111110011110100101000001 01010011000110011110110101 01010011111010110001100111 10000111110101101111011011 01001111101101010000100000 000110100010100011010000111 010000111011011111101000011 10110110100111011100101010 000101110011000111111000000 000000000110100001011011000 110011001010101010000111010 101110000001101001110110010 111011111100010001000010011 110000000011100100001010101 010010100001101100100100001 100110111011011110110001101 10011011111110000000110110
28	0100101010011001010101100101 001101111111101010010111100 0100100011000111011010100000 000110101111010010010101000 110001010011010101011111101 111011111001011011011011110 011001110111011110001110111 1101001101010010111100110111 111111111011101111111001001 0100100110001011010100100000 1011100100111110001100100110 0101001101000111000101000011 100110101100101101110110110 1101101001110010000010001001 000111010000011000010110110 0001100101001100100101110011 1000010111010111001010000101 001111001000010111010110011 0000001000011101100101000011 111001110010100010111110110	1100001111001001010000001101 00110111111101000100101101011 0111011110100110101101011010 1011011010011011100001100100 0000110000001011010101000011 111001001101000001111110001 1011100001101000101001111100 0000001010000111111101101000 1010100000110000110001010110 110001010110111010010111011 1001010111101010000110100001 100111011001111000110111111 10101100111110001010111010 0010010011000000010101100111 1101101110011100001010001111 011100001000010111100000001 0111010000111010111001110110 000011010101001111001010110 110111100000010100111100000 0101010001110110000010011000
29	00011010101111000010010011111 11110101110010111011000100011 0110000001100110111101001001 00011110000000000110000101110 1101111000001111001011011100 10110001101011100011101100101 11111101100000011000011001100 11010111101010001001111011000 010001110011010010110101100101 10100110110001010000010000101 1001000110000110011110111111 0111110111001111100110100100 110110000111010110000011000 00110111110011011000111001001 1001100010011011000010101110 01111001100011010011100111001 1100000111000111101110010110 00001001100001100011011000111 110110100101011100011011101 011001100001011110000110001011	10000100000011000010101111010 110110100100010100000101100111 10101101100101000000001111110 11001100000101001100101000000 11110111111101111110110001100 00111011010101011001101100100 11001010101001011000110001100 11111010000101100100000001100 1101100111000100111010110010 00010101100001010001100001100 00100001000100000000010001001 01011101001010111100011110 001001010000101111110101011 11001011100100111110101110000 100110101000000001001011001000 01001111100011100001110000101 00000001110111110011111001011 011111001000001000101111011 11100001100100010011110000101 00100111111111010001110001011
30	011001100001011111000101001101 110010111010010101100001010000	100000111101100101110100000111 011001001100001100100011000101

The Merkle-Hellman Cryptosystem

	011101001011111001001001111101 0111111101010011010110101100 01101100101110011100001000100 0100100001101111001110101111 10110100011010111000100011010 00000000111011101000101011100 111000101000011011001010011100 11010111101111001111001001100 100010011000101101110010001101 111001111000000100011010110110 100111000010111101101011000000 001100010100001100100000111101 010100000110010010010110000100 011010011011110110110011111010 011100011010101100000111011101 0001101101011010110110110010 10111111000000111010110001111 110110101111100101000011110101	101100001111111100001010000110 000100101110011011111010111010 110111011101001000100010111110 010101111100101011100011010 001010010010001100010100110100 000010000011001101000101111111 00001010011011111101011100010 0000110001010110000111010100 110001100101110010000000101111 001100001000010000101010011111 001101000100000101100110001001 101100000000010101110010111100 001111010110010110111110100010 101101110001001100001001011100 010010110001100110110000001110 001011010000011111000110001 000111001100000100001010010111 011100000100000101100010100100
31	111000100010000010000011110110 000101111010000001111011011101 111010011011101100010010111100 0000111000110110101110001101001 1101000110000011001011010101000 0110101000111000011101010011010 0100101001000011100010001101110 110111011100110110001110101010 1101001010000110001110011001110 0000111100111010010111101011010 1010101110010100110010100101001 1011100101110101100001100000111 1100001010100001111001011011100 111110010111100101000100110101 0101100110001101001110000001110 0111111110010111100111010011010 010010111010000000111011100010 100000000111010110101111011100 0011111110001110001100010001000 0011100100100001101001100110111	1111110000111001100100001110110 0111100001001110100100101011110 11100011001111010111101011011 1111111011111011101001001010010 000111001000010100000101011110 110000101011001111100111011010 000001111101000011110100000100 110100000100101100010001001000 0001111100010110100010000001110 0010000010101000010111101000111 1101111010001110001000011100001 0101000011000100001111011000110 1011101010001110000010010010101 100011000011110101100011011000 1100010110010101110011101101101 1101001111001011110010011101101 11001010111111100000101000101 1101111001110101010011001100011 111100110001010101101000111110 1111010100110000010101100000000
32	00000000010101111010011110101110 10100001011101100010101010011111 000010111111101100100010101100 01001100111100111001110100100000 0110001111100011000110010101100 1001001010010111001111111111010 01111110110100010000011001100000 0010010100100011110111100000110 00011101000000000000110111100110 01110101000001000100011101001001 10011110100110000001010100111110 00100001101010010111010111101010 10000010011011100110000010100101 11011001001101101111011000101101 10101001111010010101010010111010 0100100001011100011000111111000 1000110101011101011011111000000 11100100000100000001010100000000 0010101111101010001101011001110 1011000111010100000011100111011	1110000111111101110010001000101 01110001001100000101011100101100 11011010111101010101100100101010 110000110111110110101101110001 000000001000010001111101011100010 11100100000100101001000111111001 111010100101111110001010111110 10110111100110110011001111101101 0111001001110110001110100011110 1000101000110010011101111010010 0010010101011001110111110110000 01001100010101011100010101111011 11111010100110101000011000011001 01111110100001110010100000010111 01000011011001110010111011001001 00001011100101011100001010001110 100000111111100001101011110100 1000011101111000101010001110111 011101011110110000001111011101 0010000011100011100011111101101
33	111001001011111110000011100100110 10111011000111101111000001011001 011001011101000100011101100011000 011110100011001100110110111011 100101101101101010011010000110010 0111000100100101001110110000001101 111101110010100101101110100010111 110011101111101111010010000000101 01000000111010111100110110110010 01110001100011010111001001111111 101000100001010100010001100110000 101011001010010111000100011010100 10010010111101010100101001110001 111110110001001110100000011011010 001100100101100101111100000100110 10001010111111011001000111011111 010010101100101000001110100000000 001111011100100101001110111001100 11110001001100001101111110100100 110011001101000110100011100010001	110101100110010100110001000010110 0101011001100100000010111000010100 0011011101000010100010010000011101 101000011111000010111010110100110 11001010101111100010101010101111 101100101100101000101101110111000 111010001001001101010001100010001 010011101001010101000011011101011 010011000011010100010101100101110 000000000100011110001101001110101 00001011000010000110111110100101 001111111001100110000010000011000 1111111010001001010010111100100 000000100111010000010001101001111 011001101100011001100011101001001 11111100101011001010111001000000 00100111011110001000011101110000 101111001000100011110010010000101 001001001011001111001101000111100 101001001010100100100000001101011
34	1001001110011011011000001100101000 0100100110011101100100101011101001 0010100110000101001001100001011101 0010010011001001100000100111101011 0010011011110110100111001100010010 0000101011001101001010000001101100 01110101011111111100111011000100 111110101110011101100011111101101 0011110000011011111001111001100110 011010011110100101101110000100000 1000111100001110001010101111111011 111000101011101011100111001111111 0101100000111010111101110110000111 100100011111110000010101111010111 1000011011111001000101110000001100 0000111001110110001111011100101000 010011110000011111001111010011111 0010101001010001110111110001000101 0011011001000111110011011001011000 1001011010010001001001101110000010	1111110110010001111110110001111011 0010101111010000100000000001001010 1011001010110001001100101011101010 1111001101011001100110100000011000 1000111001000011011101001010111100 1010011001110001010011001110000111 0010000111110101010100000111101001 1101000100000100010110100101011011 110011000110110000111101011100001 1001101010011100011111100101110111 0011011010011111010110101010010111 00011001101001011001111101011010011 1110101110100000010111000011111111 1001111111111100001000000001110001 0000010101011110001011000001001011 1100100110011000011100110101111101 100110100011100111110101000000101 0011000101111010010101011111110001 1011101110111101100101101110001010 1110011110100000000110011100111111
35	10011000011100010010010000010101100111 001100110000101001010110100010000100 00011101010000100100111111111110001 0001100101111101001010000100111011 00001000101101110001100101001001110 00100101011110110001111010001100010 00100101011110110001111010001100010	11101011100011010010101111001011001 10110010111001000010011010010001010 00101100010001010000110011100101110 1010001010010100110100000011000 1010011001110001010011001110000111 0010000111110101010100000111101001 1101000100000100010110100101011011 110011000110110000111101011100001 1001101010011100011111100101110111 0011011010011111010110101010010111 00011001101001011001111101011010011 1110101110100000010111000011111111 1001111111111100001000000001110001 0000010101011110001011000001001011 1100100110011000011100110101111101 100110100011100111110101000000101 0011000101111010010101011111110001 1011101110111101100101101110001010 1110011110100000000110011100111111

The Merkle-Hellman Cryptosystem

	11011001110101100010001101001000100 1010100001000000001010011000101010 010010001100000000101010110110001 110110100111001101001010001011011 0111000110000101100000111101010100 101100110001100011011110011010010 001100010100100101010110100100110 1011000110110111000111010111000101 1110000101101011000000011000100001 1101101100111101110110011101100010 01011010001101000101010111101111 0010000111100010011001101101101001 00000110110011100001100011000000100 0010100011000111001100110110110111	0100101001010101111101010110011001 0110111010101110100010101010111110 1110000100100011010001111100101100 1011111011010001100001101000000011 000100010010001110010000100011110 00100100111100100110010010101100001 0101101100110010111101101001100011 01010000110110100000110010110110001 0001110101011010010001101010001110 1011101000101000011101001010011111 1110010000010001000100110111000010 0111000001100011001110000011111100 001101011011011010010111110011011 1100111000101101011000111111110110
36	100111000010111011110011110111001111 11101011101111011000000001011001010 110001101000110100010000010101001110 0111100011010101111011110001001010 110001100000111000010111101001010 01100110000101000010011011110111010 00011000001010111000001001001100000 11011010001000110101010101100101100 11110010101100101010011111000110000 000111100101100110101101000000101011 01101111011000101100110000111010010 10101010100000110110111010111010011 1011001100011111010100000101010001 0100101011000001010011100110110001 110101000011110010000101001100111001 111110000010101000110010001000001100 01001111001001001011100001001001000 01000110010000011100000110101011000 101000110001000001010011100010100110 00000100000100001111010011001001011	101100010010001111001000000010011100 01001110101000110001010101101101010 111000011111111010100101011110010 010100101000110111101100101101010001 000101000100100000000111000100101111 110000111001111100000000101000100110 0000111101110001011111001111101101 11010000110000100001010001111000001 000000001001111100000001100110110001 1000011011000100000000111011110011001 11110010000101111011100010010101101 0110111101010000010101000100101101 011011110101000001010100011001100100 000110001011010110001101100111101001 1011101101110110101111000001010000 1010110101010111010101011100110001 1010001001010100000000101000100001 011101011100101001011001110000110011 10001101011000000101010110000001010 01101100010100001010101110100101101 110101101011101010000110001010111001
37	1110000110000000010001000101101100110 1100101010010101000101101000001110111 010000001110101011100111001101000111 1010111000010001110101001110000110110 111111010010010101111011000011111010 1010000100101110011110000000000011010 100001011001110011110100010000010111 11110001100011011110101110010101000 0100100110011110001010110010111011000 011100100011100001000110001000111000 010111101010110100101000110010000111 0000100001101011101000111101000000100 0110010000101001100000100110001110101 0010010110011101010100100011010101000 0100011010110010101110000100101001100 1111000000101011010000011101110010111 100011100111001010110011101110110010 100100100000100001111010001001101010 001111010010011101111001110001011101 011111101010110100111100011001101000	1011111001100111101000000110010111110 011100110110000000011101101101001100 010100011110101111010001001101000011 100110100110001001011111000001101011 1010101010010001111011010111011001100 1111100001100111001100000101010011100 00011111001011101111100110000011011 110011111010100111101100001010111100 1010101010010101010011000011111010100 011101111010111110001010011101101000 0000110010000011011010101111011011001 1111111101001000100110000101000101100 0100100100000011110101110111010000011 111111000110101010001001011001000001 011110100000010111110000101010000111 0100101011010011010011100100111000000 0011100111110101110111110111100111000 0011010101000100000000011001110011101 01000110111100011111100000000100000
38	01000110001110011101100101100101011100 01010010010111010001110100000001110001 00011010100010010010011101110111101110 10010100000001000001110010111111101110 11001000100101000101111100011101011110 1110101011111101110011011000000101111 10010110101110000011101011000100011111 10100100011011111110010001010100001110 01010000100011010100010010000100001010 10110000101011000010010001000110100010 1100011010001001000001001010111011100 110111000110101001010100011110110100 100110011010110110000111101101100111 10001001111011100001010111100101101001 11100100010001010011001100011100111001 11011100110100110101001011001001101101 110000110111100111011100011111111110 1101111100000010010001000000001001011 111000111101110110001111011100001101 1001010111011001100000111100000001101	10011010111001111000001110011011110000 1001001011111011110011111100110010001 00000100101011001100011110111001001000 00010000110000000110000001001010110010 010100101101110110110011010000101 0100010001101000011110001101000010001 0010000101010100000101000011110101101 0010000101101011100000111111110100110 00010100001100111010111001000111010101 01000010111011111001000111010101 0100001011101111110100010011111111000 0100000001100001100101110110000101101 110001100111001000010001111101110111 001111011110000000010010100101110000 10100100111010111010111010001111011 100011010110011101010111001101100011 000111000101111011110111011100000111
39	111001011110111100111100100100000101001 11001110101111101001011110010100110100 01100010000100111001011101111000011000 0000100001111010101100101111011001100001 100011101100010010101010001110011110011 0100100001101001000101001101110001000101 1101010110001011111111010100111010110 100001100101111011111010011110100111100 111010101010011111001010011010001010110 011110010100010011110011100010000000110 010000111010111000100010011010110101110 11110111111101010100001101011010110001 0011110111101111111101011000111111100 100000111011011010000011000001000100000 110011000000000001101010001110001010101 1101111101111000110011111000101000110 101001101110111001100000110101001011000 1011000000000000100110100010010010011000 10011111110011010111010101000110101111 10100001100111110100110011111001010111	110111101110001100000100101100010000100 0110100000000000111000100010011010101000 010011001101011111001101000000000100011 001000100110111010010011100110000000100 100001011000110111000110001000100110000 1000110101110011011110011100001110110 10101100101001100000000100000100110011 101000100001001001110001000000110000001 01110011101100001110010010010110111100 011011010111101100001111110111000100 011001101010001111100101100110011100001 00010011101010101010111111010000000111 0100001011110110101010010011100000010 11100000011001001110111111011101100001 1110001011110000010100010001010100001 01111010111010111011000101100101101110 011110000011100110010001011000011100011 11011000001010000011111011100111000011 01000001110011010101001001100001010001
40	00111010011001000001011011110110101101 101010010101001000000110101101110011001 10010011111110110101000001011100110010 1010111000111101110110100010110011110111 00010101100100000001110111000000110011011 011110110000101100110000010111100101011 1101000111111100101111000010101101111 0001011110001101101100010101101001100000 0100101100000101001011110011100000001010 001111100000100111111101000000001011101	0001101110100011011000010101010010001000 001111101101101111001110011001000000011 10001010000001100101111111110110011001 01111010110001100111101000010111101010 00000010000101011011010000110101100110 001001001011001100000001011001000111100 110000011100101111010111111100011100111 011111000100000001000111001101001101011 1010001000110001101100100100100011011000 101100110110000010101000001011001010001 1010001000110001101100100100100011011000 1011001101100000101010000010110010100001

The Merkle-Hellman Cryptosystem

	0001010111011011011001111011010100110011 1000000111101100011001011111010110010110 1110110010001010100101001000011100000110 1010000010110101000110011000000110001100 01001111010110000001010100001011111110 0000001110111010011110011110001001000011 110100010011011001100001111111001010110 011110101000110001011101011101011101011 100101101000011101010100011000001111010 1000111010010001100111010101011101011	0111101111011011100010100010100100010111 11010001010010101100001100100010101010 001111101100001011000010010101010101011 1000110111111110101100101111100000101 000011101011100101000101101000101100001 01010111010111000100010100111010010000 01011010011010111100010100001011000100 101010101110111101110011001100001100111 0010000011101111001100001010011000001 0010010011101100001110100001011111010
41	0110110110101000011110100001111010101101 100111100110001110110010010010011001000 10110101000101111101111101111010101011 0110011010010110110010010001100000000001 0011010010010111101100000110100000010100 0101111100110111011000111100100000010010 1010110101000111000000101010100100111010 01001110111101010001101001010111011001100 11101101101001111111001011011010111001 10110111111111100011000110010000110101001 001100100101011010011101101010101010111 11011110100111101100000100000100101010000 00011101000011000011011101110010001000111 01001011101110101110101110011110111011 1101101010111010011101001101010000001011 000111111110101111111001000010011010110 010110111001111100011111110101011110100 1000011001000011111010111100111000110010 011010010100011101110111111100011000011 00001001101101110111011100000010101100	10110100100001100100001010010011111010100 11101101111011000111111100010001110000111 10011011011001100101100000000100010001111 101010010110010101110111001111001011111 01010111110000101100110101010011000010001 0111010001010000101010001111010000111011 00101001011010110100110001100101000001010 100110101000001001000110000111100001 10011011111100110110010110001000010111 00111100010010001010001101001110011010001 000000001110010001110000110110100111111 100011001111001110110000000001110010101 001000000100000101110001000011000010111 11010100110000000011000011111101100001 11111010010111000000001100001111110110001 001110000001000001001000111000110100100 001110000001000001001000111000110100100 1111011111010100011011011011111110101 001010011100110110111000101110001001 011001010011101011101010100010101001101 010010100111010111010101000101011010 01011001011101000001010001011101011010
42	10010100000011011011111100011111001101000 1010011011010011111110011111101101010010 0001111011110110011111110100111111001100 10000000100100101000101000010111000110100 00001110001010100000110000010000011100101 10011111110010010010011101111010011110001 00000111000111101010100001101001110010101 1001100001100011110101010010100110011001 011010100011010011110101010101010010111 0001001110100111110001101101000101110111 00000010011000001110010001000010100110000 11010000011011000001111011111000111001000 01010110010101010111011000011100010001110 00111100001011110000001000011001111101110 01101001010010000101010100010000010000001 11110010011001101100100010101111110000100 11000010011011101100101101100110001000010 0111001010010010011000100001111110111010101 101010000011100001111001001001001000110001 00101111010111110111110001010010111101110	001110001111001011100101101000110001010000 011111010011000000111001000001110011111000 10011111000001011001000010101110000110001 101000001010111100110001011011000111001101 11110001100000110001110111101100101110000 10001011110011100001001011111100101111101 11000000110101011100010110100011101001011 001011011001110001111001011010001010001000 10011101000111100100111110111010000111110 10010111100010000010000101110010110111011 10010111100010000010000101110010110111011 10011111110111110011001010000100100110100 01011100110001001100001101000101000110100 00011101001100000101101111010010001101010 0100001111011000110000010000000100001111 111011110000100000010101110100000101000 000000010010110001111001011011111010001000 00100111110010001101001101110101111001001 00100000101000011110001101111100001100100 10111010000101000011111100010111101000011 01010101110101111010001000111011010111101
43	1101010100110011111001010110000100100001010 0110111011010100100101101000101101101000000 0010100111011010000110111100110001001000011 0001101010001000000011011010100111010110101 0010011000110001000001110111100011101011011 011011000100010001110110100100001111011000 00011101010100000010001000111010010100101001 0100100010100001000111000000100001111110000 0100000111000000001011100110100101000001011 1110011000101000000100000001010101001000001 0101011000111001010011011110100101001001111 0100000001010111001100000110000101010111011 010110100000001101001001111101101110110100 100110011111011011100010110001111000111011 100111011001110001011100111011011000101100 00101101001010001011100110010111111000011 0001111101101010011000001000110100110110010 1010010000100011000110101110110010100100010 010111100111101011001001111001101110001010 100101101000011111100000100100111100110111	0111000110011000000000110110111001000110110 1001001101100010011111001000100011011011101 010101111011000110010110010101101100001111 101110001111000011110101111000000110000001 1101010001110000100011001011000010110100011 0001010110000000011001100010000101001000001 1010010100110001011111100100010101011001 01011101101000011101111101101000011001100 01111001000001001010101010111011110111111 00011010111101000000010110000000111111100 11001100110110001000000101100000001111100 0010101110011110011010001110101101000111011 11010000101010001100110110001000000101111 111011100111001010011100110011010111011010 001100010110101010111000110111100011001 0100101011100101110100001110101100100001101 100000010001101100000111001000101100011101 001001101011110011100011011111101001001 1001110111100010010010011001100100001110110 110111100100110100010011001110011000010000
44	0110101100101101011110011001001011111101010 10000010010101110001011101101001011011001001 0010010111100100100011011000001001110110110 00110001010110101011010011101100001100010001 1001111001101010111101110110011011111001001 111100101110110110010110111101010111011011 11110011100010110010110001011000110010010001 1011011010000100001101010010010101100110110 0011011100001001110000011001100100111100010 11111010111010101111010010010010011000011 0111010010001010100010100101100101011001111 01011101001000111101101110101001100110000 0001110111110000110011001001000110011000111 1110000011110001001101100110101011011101111 000111010111000100001011101111100000000100 1000101010011011111001011001000110110111000 000101110001000001100100101110011011110010 101100111000100101000010100010000111111001 100100011100000010101100111010000010100010 0001001110110011001100110011001100110011001	000101110111100001111111011001111111101100 000110110001110010111110001011110101011101000 00101101010010111100110101001000000100100010 1011101011110111011101010000100111000010010 01011010100111010001001110010101111110000100 01000000001101010110010101011100001010000 0110011001100111001010111110000110001010011 000101011101110101011101010001111100001010 100011111001111100110001011100000010100000 0001001100001001110100000000100100011000100 00101001000000000111100011100111011101111 110101000101010001100110110001000000101111 111011100111001010011100110011010111011010 001100010110101010111000110111100011001 01000001011100101110100001110010010000011 11010110011101000001001010101111011111011 10001001111011110011011101010001000100101 1111011101011100011011001111110101000100 00010110001110100101111101110000101101001101 11110001111001000110100001000001001000000001
45	10110010110100111100011110110001110000011000 10111010011001111110011001111110110010111100 00101100101100100100111100011111000011000101 011110011101100110001010001010011010101101110 1000010000100000100001111110100000001010001111 111000001100100000110000100101010111010010100 11010001100000010000101000000001001010100100 001110101101001010010001000100110000001001101 0100011100000111110001111101010011110001000 0100001010000000110001111000110101110011110 01110010011000111110010010011110010011100001 011100011001000110100011011001110000011010101 001010011000101101001111000000010000010110001 1111101001000000011011000100101000101110100100	0010010010010010010000011011010111001001011110 0111100101001101111110101110001011110101101 0010011101001100000001000110010001010001001001 01110001110100000111111001111100001111110000 011001110101010100111011101100010000000100011 11010010110000001110001010111010011000010101 01010110010010101000001101000010101000101110 00010001110111001001101100111100010110000110 000100111000010100100101011100010110000011 100100010100011011010111101010110001011000100 01010010000111010011011010101001100110000100 1100101100111001101100110110000011010000011 101100111101101000100001010011001100011101100 00100001011101001000101000010100011010110011 00100001011101001000101000010100011010110011

The Merkle-Hellman Cryptosystem

	010100010111101001000111000011000011100011101 111101000111011110101110001101010011111 10110110100110000100101000101011110001 00010000110101010100100000000010011010 00011001011011100100110111001000100011011 0000100110111100001010011110101101001101	0011001110010101010001101010100111101110110 11010101000110011010011001001001000101110 01010000000001110101010011101010101010 001101001111011111010100001001000010110 11101100101010000110001000100010100111 0110110100111010101111001001100100011110 111100001101010001010001110011000000100111 010100011101100001010000011101100000011000 0101000011101100011101001011101100001111 1110000110100010000010100000110101101010 001001101110001100100001000001101011100101 110000000100100001110101000001100000110011 1100101000001111100000110101010010011111 0011011010110011010101010001000100101001100 011011101001100111010100001111010101001100 11000111101010000101010100000110010100011110 100100011010100011101100001100110100101010 0100010010000000010000010010000101001100000 01010011011111101001101001010000000001000101 101010011000101111000011100101110010001000 11110001011011110101011011001000010010111 11111010101111100001110101001111100001110
46	0101001010010100001010011110100110100100110 010101111110101011101011111010101010011 000010011000000011010101011000010001011100 001010100100100100001010010101010100001011 10100010011010100101001011010111101111001100 0100011001000111100110101010010101000101100 110001100101010010111010100101100110100101001 000111100111100110101011110000001101000110 001001101111000111001000010000010101011100101 11000000001001000011101010000011000000110011 11100101000001111100000110101010010011111 00110110101100110101010100010000100101001100 011011101001100111010100001111010101001100 11000111101010000101010100000110010100011110 100100011010100011101100001100110100101010 0100010010000000010000010010000101001100000 01010011011111101001101001010000000001000101 101010011000101111000011100101110010001000 11110001011011110101011011001000010010111 111111010101111100001110101001111100001110	1110110101010001100101111011110110001100001 10011110000010000110000001001100110101000010 100010101001010011010101010101010000100001000 011101000111011010111110010011001000011110 1111000011010100010100011100111000000100111 00101011101000111010000011100111010111011000 1100111100010111000001011100101010100010010 0100100011000000010001001011000111001010100 10110001001000111000010100000110010101001 0100000010000101001001010000110111001001100 0011100001110000010000010010001110100111011 000001110011000111010011110010101001111011 010100110100001110110111011000110010000000 10101000000010110101011100100101011010000 11000010100100110100101001011001101000000 0101100001100111001010110010000101011010000 010110000110001100010000001110010001010111 01000111101011100010111001111100000101011
47	1011001011001000111010010111101000101000010100 111011101000011011000111100001001111001011100 10111010101001000011110101001110011111010111 110111101001000001010111001101001000000000101 11001110011101001010011001000101010101000101 11000001100100000100010001001010111110010010001 110000111001111111101001010010010001110000011 001001111110000101001101001111001101000000010 1001001001111100100010110101110101111011 1000010100100110000100101101100110011101100010 00011001000110000011100111110101001100111011 000011001111001111000011110010101110000100 100111001001000111010101011001111100110100000 01010000110110001000110100100110000001000001011 0100010010100000010111010000110011001111001011 110101001010011010110010000100100000100101110 0100010011100011010011110000010001010100101 1011101000111110010100001011101001100010111 1010100101010101011110101001111101010101110 10000111001011100011101001011100111011011	1110111001100100101010001110100110010100100001 10011100011101110101011000001101111000011010 1010100101111010111101100000001001000011011 01000100001101000001000101010011101001110100 10110000100100111010100100000111101001111000 0111100000111000101010111111100101010010100 0111000011100101110101111001001000000001010101 001010110011100100101000110010011110000000010 0100010011010000001110010010100000101001110 0011101011100100001011100010111011110101010 0101010001000000010100011101001011111010101 100100110000110010101010011001000000100100 11101110110010011010000101000100100111100110 010111000011001000001010111011110101010111 01000001100110011001110101001011111010111 010000010101110101000010110000010110101010 0111110101010011110100000110010101001100011 010101000000110001000110011011100101110110 01111000100010101000000010100011110100100100 1000010001000010000111101000101001101010101
48	11100110011001100010100010000100100100011010000 001011011000110101011110101110100011101100110 1110011110001111011010101111010101011110111 1111010001111000110011111001110001110010100100 010101110000000000110010101010100010101001010 0010001101011100110101110011001001010100000100 1110101110000001011000001110011001101111011010 1010000010000100011001010000000010100000100111 0011110001011001011111100110010001001000111011 010010111010110001101011111010111011000111001 1110001010111111111100000000100010100000111010 10010010100101001000010011101001100101010101001 110101100110011101000110101000010001101100010 11110110011110101011110101111000110101001000 00000011000111101110101010011010010011110100100 111101111010100110100110011010010101011001010 00110011011100111010011111010111111010100000 10001110011101100001100101010001101010011001111 11100101101001000001110010110010110100011001111 0000101100000100011110111001110100001110010110	0000001111100101010001101000111110101111010101 01001100011100010100000011110000110101010011000 0000111100010100010101000100000101111010100 01110011110000100000000100011100001111101010000 10101000100101010101000100110100010100100110001 10000101011000000110000100111110101011100000 0001110101110110001100101110011001000110001011 100010110000000001111101100110011101110001010 110101111010011010010001010111101011111010100 011110111101101000001100110001010101111100 001010111001110111101100000101011100000101011 01111010100101010101110100101011110010010111 0101111101000101001111010100011011000111110 0001011100001010001010110000111011110010100 10000011101011000010000001010000010100011110 00101111011000010100110000101010000101001110110 11010111011111110011111010101000101011100110 1010011100000101011100101010101010111010101 00110101100000001010110101011010011110010101 01100010100100100000100010100101000111101010000
49	0100110101100011011100001001000011000110100001101 1100010100111110100011001011101100110101010101 1110010110111110100010011110011100101001101010 1001011100010010001010001101010000001000101110101 101001100100010111100000010010000011101011110 0111011000010101000010111010000110101011101000010 001000000110001110101110110100101111000001011 001110100100001010010010101010100000101001000010 11011010010101000100010011100100000010101011010 00001000111110011001010101000001001110000100 1010000110011101010010110100101110111010011010 011111010100101110000010010111111001010001111 11001100111000111010010101000011010001011000001 011011111001010000011001111010100010001101110110 110011110100011111011101010010101000110011110 010010000110001000110101000110101010000111110100 1111010000000010111011001010101000111100101000 100011110010100010110110100000001010000000100001 010101011100010001111101011000100011110001010001 00011111010010010010100110011101101101010000000	100011001010010001011110101111011101100011000010 100100101000100111000000101000110101111101001 01111000100011100001001010100010000100011111001 0011000001010000100110000011101010001111000110011 001000010011111111000111000010101110101011101 1101100110000101010101001010011101001110101000 01001011001010100100010001000101000111001000000 01010010011000010000101010010001110000010111010 0011110100100010101000100101110100000010101111 010000101011110010111000101110000100001011011 00000010101110001001110100010101110000001010001 0111111011110101110011001110001100010000001010 0100010001010100100111010001010110000001010001 01111110111101000110010101110000111111000101 01010001000110010001100110010111000001100100 0101000101010101000000101101010110101010001011 1011110001001100001110000010101101000000101001
50	110001101110101111110000111001000000001111000011 1010001101100111100111000001011001111001111001110 1110010011100110101001000011010100001010010001011 001001101010101110110111111101100100100100001 000011111111100100010010111011000101010000101110 0101110111001100110001000010010111110001101001101 00100010111000110100101001000011111110101010100 0111100110101010100101001001111110011010111111 101100001001000000110100101100000110000110111010 1110000111010011111000111110101111001101001000 00010110010010100100100101111000010010110010110 100110101010100011100011101001110011110000110011 111001011001000100100100010100010100000101010001 11111111000010100010001000100101101011110100011 11011111111101001000001001111001001000011000101 00100010100111001110100100110001011101111001001 0100110000000100110101110100010011000000010101001	100100100100011100011101010001000111110100110111 00111111001010101111001010011001010010010000100 0101110101100000101010111110000001110100101111101 11101010010100011110100010111000101010001100011 0001001001001111000000111001010011110010101001 001110110011111011100111010001010111110101100 10011010100110000100000010100110101010100110111 01001010100110001000111111000110101100000101001 010110001001100100110010001010100000111110010101 110101000101001101010100001100100000011101010100 1001101001111011000110010101110000111111000101 010100001000101010101111111010101110010101010 10101111001111011000011100111000000011001101000 000101011001110011001010010000000101111101100 11110110010111011100000111001011010010111110000 10011010001000001010001001110101010100000101010 01010000111010011100010110010111111010101001010 000111000010100011110010001100101110010110000

The Merkle-Hellman Cryptosystem

	100011100000001001000110111100010010010011000110 11000100110000011100001011101001001101100110001	101001010100001100111110110010101100101110000011 00000001110111000001011011101001100101101111001
51	110100001111001001101011110000110011110110011101 110011110010001010101101000001010111110010101110 0000101111010101100100000110110011100010010001000 111110111100011100100110001000010000101111011000101 00100010001001101110010011000101000100111101111011 101000111010111101000111101010000110011010110000 10111001010011001100000000000110110011010100101 11001011110111101101001100011010011000001101000 01110011101010001000110011010111101110100100010000 100111001010110110101001011110110000010001101010 01110110001001111000110001000010110110010001110 110101001001000111110110100111000111000110001000 110000100011001011011001000110000011010000101011 101010010101101001011100100100011100101010000111 100001001111011101110011100111000000111010100100 000101101111101000110100011010111110001001110110 1010001000000010111010000011110111101001111010101 010100111000100101100101111111010010111001110110 00010001001111111000110101001101101010110100100001 0100010000110011100001011110001111010001111000000	00111111011110011001100110011100101010010110010 0000010011011111001001111001101100111100000010 1010011011000001101000000110110110001101100001010 1010010010110100001000110000010001110001011011 011110010100101111000100110010100010000100000000 101011100101111010100011100010111100001001101 10110101001010011010011100110001101010010010000 1011000110000100010110011110100111000011001101 001100001100001001011100010101001011010001110111 010001100000011011011111011001100000010011011 00010000011101111100000100000100100011101010 110011101110110111000010001011011010000001101010 1100111011101101110001000101111010000001101000 10101001101101001101001101010101111101010011 0011010111100001010001110001010000010011000001100 101010110110101001100011000100000100111101000010 10111111110101011010010100001010110110110010
52	011101001110111110010000100110100010000011100101011 101100110100011100001000001010111101010111000001 100101001101001000011110010001000010101101001010010 0000001011010101010001111010111000111101101111100 001011011001011100001011000011100001111011101101 00010110100001011010001000000101000100001111010110 00101011110100000001100000001101000000010010011000 00110000011010110010011000111111000100011110001 100001000010010010101011010000000101101110101111 0101011011110011100110011001111001110101111000 011110000100000010001011001010000101010110101010 0111011100001100100111101111011001101000001111011 1001110001111011101100001011000010100010101001101 101010111010001111001001010110011110011110101100 0011000100011110100100110110000100000001010010001 0001010111101011010101001010001101001001110011011 111110010101001001000001000010110111011101100001001 11111000110010100111101010100000101010001110110010 0100001101001101100011010100000111100000000111010 0110101101101100001000110000100010001110010001111	0001000101100011000111100001100110110001111100101 0101101001101110110001100001010110110010000010101 010110010001000101111110101010000000011100111101 001011001000101000111001101101000000011000011000 00011110100000010010100001011000111011001111010011 0001110110101011110100000010100101001101001000001 000110100000001001100000111011010100001010110101 011101111100100001000110000110110010110101101011 10111001111100101000011001101001011111010100001 1011100011000010000100101001001111011010100001111 0001001000011010101000010110000111001011100011010001 1100110011000110001000111101011101000100011010011001 0100110100100111000101010001001001110000100000110001 010110000100011100011100011110110001000011110111 1010011100101110000101100101100011000101001001010 10000010000100011101101100000010100011100110101010 11011110000101010000110010100000010011101100110101 01000101000111101101000000010100001110111000001 000000100111100011011010111101011101100110010011 1010100110101000010001100001

The Merkle-Hellman Cryptosystem

	10101110111101110100100001010111100110011000101000111 10010000001110010100000011110011000010010111101001010 1101100101101001100010000100100100111111011010011101111 1100010101000010100111111100100110001000011111110101 0100110010000001110101110011000010100000001001101100100 111001011000010100001000000101111001111011000000110001 00010101000011111100100110010101001000111111011000000 1001110101011010001100100001101001001101010000001110 0001010000101000011000110010101010101010100100111001 1101111010110000100111101001000101010000100010001000 111101010110011111010000111010010010011111111100010100 01010100100011110101110011000101001010000000000100011 110001000010101010110100010010010011111011111001010 0001010110010010000101011110010010000010101001000101 1001000000101000000101001000010101010101010011001110 0111001010000101001110101011110000100011110100001110 11011010100100010001010101101010101010000010100001101011 010110010100000010010101001100010010011110001011	00111000101100111010111011001001011001011011000001 0111100100101011111001011010000100010010100000100010101 010000111001011001010101001001001001100110001000101011 00111000000101011010000001111000001110000011101101001 000000000010000110001101010010001010000111101000100000 11101010110010101001111100100001011010111001100110011 10000011101110110010000001000101010011101001111000010 001010101010011001101010011010100110110001110101010000 1111111100110000001001001110100001001001010000101000 10011010111000010010011001110011111010001011101010110000 010111100010101100111001110000010001010101001000010000 100110001001101000101010001010010010001000010000100 0011101000101011000111001011110100010000100101100 00111101001001101000110001100010101000010111010101 00000100001010111010111100110001100110001000000001001 10011101010101001010110100001010000010110111001011 0101101001000100101010101010100000100101010100010000 10000101001000101111010001010101000010101010001001010 10110011110000001011001100010010010101110101100101010 10010000000010001101010101000010101111111000011001011 110011001000100110011001010010101011000010000010000 0001011001001100111011010010001100110001010100010001 0001100110100001111010011101010011000000101110110000 111101110110101010000001000010001110001010100111001 000111100100110011001100000011101100010011010101011 011011000100110011001000001110110010011010101011 00011000000101000100001000101010111101000101010101011 00010000001010001000010001010101111101000100101011 11010111011110011010101100000100100001000100010010 001100100010111000101001100100100100010010100010000
57	0010010100110111111101011100101010010011110001001010 010000101010111011010000011111010110000010010010101000 0010111101100101101101001010001100000000010001001000101 1010100000001000010101111110001001100111001000010100 0101010011110100001010010001110000010100000100011000 1100100101011011000001001100000101000110110101010000 01001100000111000110000011100101101001010111010110000 000000100011011100101111001100101001010101000000100111 0001100110100001111010011101010011000000101110110000 111101110110101010000001000010001110001010100111001 0001111001100110011001000000111011000100110101010111 011011010010101100000000010001010000001001010110100 000000100010010010010101011010011101100100111010010 101011110111100111010101100000100100001000100010010 00000011100000100111010101001111010010001010001111 01101101000010100001000010101010001001011111000010110 110001101100000000010000111000111011000101010101011 0001000000101000100001000101010101111010010001011 11010111001111000101001100100100100010010100010000 00110010001011001010000101110101010111000001010010	0010101000100000010011111010111010001010101101010101 000101111011111000011111100000100100110110010101011011 0110010011100000010010011110000100001000111011101000010 0011001010111010000100110101011110010101010010110000 10011101010111100001010101011010111010101101001010010 01111010000000010111010100010101011100100010110110001011 001101000100001111110000111101000010101010101010010

The Merkle-Hellman Cryptosystem

[illegible]