TRABALHO FINAL

NOME: GABRIEL ALMEIDA MENDES DRE: 111204959

(1) SEJA $m = 3 \times 2^K + 1$ COM $K > 1000$.

O TESTE MILLER-RABIN EM TODAS AS BASE POSSIVEIS $b < 20$ DETECTA QUE m É COMPOSTO.

ATRAVÉS DESSE FATO AFIRMASSE QUE $256^{1536} \not\equiv -1 \pmod{m}$.

ISSO SIGNIFICA QUE DADO $b = 256$ E $m = 1537$. m É COMPOSTO PARA A BASE b. REALIZE-MOS O TESTE DE MILLER-RABIN PARA PROVAR SE ESSA AFIRMAÇÃO É VERDADEIRA E m É COMPOSTO.

RESULTADO:

$m = 3 \cdot 2^K + 1$ $\qquad \frac{1536}{2^9} = 3$

$m - 1 = 2^K 3$

PRIMEIRO FATORAMOS A MAIOR POTÊNCIA DE 2 DE $1537 - 1 = 1536$. QUE É $1536 = 2^9 3$

EM SEGUIDA CALCULAMOS A SEGUINTE SEQUÊNCIA MÓDULO 1537:

$$256^3, 256^{3\cdot 2} \dots 256^{3 \cdot 2^9}$$

I - $256^3 \equiv 861 \pmod{1537}$

II - $256^{3\cdot 2} \equiv 861^2 \equiv 487 \pmod{1537}$

III - $256^{3\cdot 2^2} \equiv 487^2 \equiv 471 \pmod{1537}$

IV - $256^{3\cdot 2^3} \equiv 487^3 \equiv 364 \pmod{1537}$

V - $256^{3\cdot 2^4} \equiv 487^4 \equiv 513 \pmod{1537}$

VI - $256^{3\cdot 2^5} \equiv 487^5 \equiv 837 \pmod{1537}$

VII - $256^{3\cdot 2^6} \equiv 487^6 \equiv 314 \pmod{1537}$

VIII - $256^{3\cdot 2^7} \equiv 487^7 \equiv 755 \pmod{1537}$

IX - $256^{3\cdot 2^8} \equiv 487^8 \equiv 342 \pmod{1537}$

X - $256^{3\cdot 2^9} \equiv 487^9 \equiv 558 \pmod{1537}$

OBS: O COMPUTADOR FEZ ESSES CALCULOS, EU NÃO SOU MALUCO.

COMO O PRIMEIRO ELEMENTO NÃO É CONGRUENTE A 1, E NENHUM DOS ELEMENTO DA SEQUÊNCIA A 1537, ENTÃO A SAÍDA DO TESTE DE MILLER SÓ PODE SER COMPOSTA.

ENTÃO $256^{1530} \not\equiv -1$ É VERDADEIRO.

(2) SE UM m É PSEUDOPRIMO NO TESTE MILLER-RABIN PARA A BASE b, ENTÃO m É UM PSEUDOPRIMO NO TESTE DE FERMAT PARA A MESMA BASE.

RESPOSTA:

TENDO COMO REFERENCIA MILLER-RABIN, TEMOS:
COMO m É IMPAR, ESCREVEMOS $m-1 = 2^k q$, $k \geq 1$ E q É IMPAR.
SE m É PSEUDOPRIMO EM MILLER-RABIN PARA A BASE b ENTÃO
OU $b^q \equiv 1 \pmod{m}$ OU $b^{2^j q} \equiv -1 \pmod{m}$, ONDE $0 \leq j \leq k-1$.

- NO PRIMEIRO CASO: $b^{m-1} \equiv b^{q \cdot 2^k} \equiv 1^{2^k} \equiv 1 \pmod{m}$
- NO SEGUNDO CASO: $b^{m-1} \equiv b^{2^j q \cdot 2^{k-j}} \equiv (-1)^{2^{k-j}} \equiv 1 \pmod{m}$

NOTA-SE QUE: $k > j$, ENTÃO $k-j \geq 1$ E PORTANTO, $(-1)^{2^{k-j}} = 1$.
EM QUALQUER UM DOS DOIS CASOS OBTEMOS QUE $b^{m-1} \equiv 1 \pmod{m}$.
E ESTA FORMULA É JUSTAMENTE A SEGUNDA VERSÃO DO PRIMEIRO TEOREMA DE FERMAT, BASE DO TESTE DE FERMAT. LOGO m É UM PSEUDOPRIMO NO TESTE DE FERMAT PARA A BASE b TAMBÉM.

(3) SENDO $p < q$ DOIS PRIMOS.
SUPONHA $m = pq$ E DIGAMOS QUE $p-1$ E $q-1$ AMBOS DIVIDEM $m-1$.

(i) MOSTRE QUE $m-1 \equiv p-1 \pmod{q-1}$ E OBTENHA UMA CONTRADIÇÃO

RESULTADO:

COMO $m = pq$, TEMOS: $m-1 = pq - 1 = (q-1)p + (p-1)$, PORTANTO,
$m-1 \equiv p-1 \pmod{q-1}$.
COMO $p-1 < p < q$, TEMOS QUE $p-1 \not\equiv 0 \pmod{q-1}$. ISTO É
$q-1$ NÃO DIVIDE $m-1$, ACHAMOS A CONTRADIÇÃO DO ENUNCIADO.

(c) CONCLUA QUE UM NÚMERO DE CARMICHAEL NÃO PODE SER O PRODUTO DE DOIS PRIMOS

RESULTADO:

PARA CONCLUIR ISSO, PRECISAMOS USAR O TEOREMA DE KORSELT.

(4) $n = 938957$, CHAVE PÚBLICA DE RSA

a) $\phi(n) = \underline{937020}$. DETERMINE A FATORAÇÃO DE n.

RESOLUÇÃO: PEDIR A FATORAÇÃO DE n É O MESMO QUE PEDIR PARA ACHAR OS PRIMOS p E q CUJO O PRODUTO DÁ A CHAVE n.
• DÁ PARA ACHAR FAZENDO UM SISTEMA

$$\begin{cases} p \cdot q = 938957 \\ (p-1)(q-1) = 937020 \rightarrow pq - p - q + 1 = 937020 \end{cases}$$

$$938957 - p - q + 1 = 937020$$
$$-p - q = 937020 - 938958$$
$$-p - q = -1938 \; (-1)$$
$$p + q = 1938$$

NOVO $\begin{cases} p \cdot q = 938957 \\ p + q = 1938 \rightarrow \underline{p = 1938 - q} \end{cases}$

$$(1938 - q)q = 938957$$
$$1938q - q^2 = 938957$$
$$q^2 - 1938q + 938957 = 0 \text{ (RESOLVE EQUAÇÃO DE 2º GRAU)}$$
$$q_1 = \underline{967} \rightarrow p_1 = 1938 - 967 = \underline{971}$$
$$q_2 = \underline{971} \rightarrow p_2 = 1938 - 971 = \underline{967}$$

OS FATORES PRIMOS DE n SÃO 967 E 971.

b) O MENOR VALOR DE $d > 0$ PARA d SERVIR DE CHAVE SECRETA.

RESOLUÇÃO: PRIMEIRO É NECESSÁRIO ESCOLHER e QUE SEJA INVERSÍVEL MÓDULO $\phi(n)$, OU SEJA $mdc(e, \phi(n)) = 1$. NESSE CASO, $mdc(e, 937020) = 1$. QUE NESSE CASO ESCOLHI O PRIMO 29. PARA ACHAR d ELE É INVERSO DE e MOD ϕ. O MESMO QUE:

$$29d \equiv 1 \text{ MOD } 937020$$

NESSE CASO É FÁCIL POIS DIVIDINDO 937020 POR 29 DÁ:

$$937020 = 29 \cdot 32311 + 1, \text{ DONDE}$$
$$1 = 937020 - 29 \cdot 32311$$
$$1 = 937020 + 29(-32311)$$

LOGO O INVERSO DE 29 MOD 937020 É $d = -32311$.

⑤ $m = 19291$

a) CONTRUA UMA CHAVE PÚBLICA e.
DETERMINE A CHAVE SECRETA CORRESPONDENTE.

RESULTADO:

PRIMEIRO FATORAMOS M PARA ACHAR p E q, USAREI O ALGORITMO DE FERMAT,
COMO $\sqrt{19291} = 138.892$ NÃO É INTEIRO, USAMOS A TABELA

x	$y = \sqrt{x^2 - m}$	INTEIRO?
139.0	5.477	X
140.0	17.578	X
141.0	24.289	X
142.0	29.546	X
143.0	34.029	X
144.0	38.013	X
145.0	41.641	X
146.0	45	✓

LOGO OS FATORES SÃO:

$x - y = 146 - 45 = 101$

$x + y = 146 + 45 = 191$

PORTANTO,

$\phi(m) = (101 - 1)(191 - 1)$

$\phi(m) = (100)(190)$

$\phi(m) = 19000$

PARA ACHAR e ESTE TEM QUE SER UM INTEIRO POSITIVO INVERSÍVEL AO MODULO $\phi(m)$, EM OUTRAS PALAVRAS, $mdc(e, \phi(m)) = 1$.
PARA ESSA SITUAÇÃO PODEMOS USAR $e = 3$.

AGORA PARA ACHAR A CHAVE SECRETA DE (m, e) QUE É d, FAZEMOS:
$ed \equiv 1 \text{ MOD } \phi$; $3d \equiv 1 \text{ MOD } 19000$. AONDE $d = 6333$.

b) CODIFIQUE A MENSAGEM 12345 USANDO (m, e)

RESULTADO:

$M = 12345$ NA CHAVE $(19291, 3)$

$M^e \equiv a \ (\text{MOD } m)$ → SENDO a A CLASSE DE EQUIVALÊNCIA

$12345^3 \equiv a \ (\text{MOD } 19291)$

$12345^3 \equiv (-6946)^3 \equiv (-6946)^2 \cdot (-6946) \equiv 48246916 \cdot (-6946)$

$\equiv (-19166) \cdot (-6946) \equiv 133127036 \equiv 17746$

$\equiv 17746 \text{ MOD } 19291$

(6) SEJAM p E q PRIMOS ÍMPARES, COM CHAVE DE CRIPTOGRAFIA (m, e), ONDE $m = pq$. PODE ACONTECER DE UM BLOCO b DE UMA MENSAGEM SEJA CODIFICADO COMO ELE PRÓPRIO NESTA IMPLEMENTAÇÃO. OU SEJA, PODE SER QUE $e(b) = b$. UM BLOCO CHAMADO INVARIANTE PELO RSA COM CHAVE (m, e). DETERMINE QUANTOS SÃO OS BLOCOS INVARIANTES PELO RSA QUANDO $p = 3$, $q > 3$ E $e = 3$.

RESOLUÇÃO:

A EQUAÇÃO $x^3 \equiv x \pmod{p}$ TEM TRÊS SOLUÇÕES QUALQUER QUE SEJA O PRIMO $p \neq 2$. DE FATO, SE $x \not\equiv 0 \pmod{p}$ ENTÃO $x^2 \equiv 1 \pmod{p}$. ESTA ÚLTIMA EQUAÇÃO SÓ TEM RAÍZES CONGRUENTES A 1 E -1 MOD p, COMO VISTO NO EXERCÍCIO 8 DA LISTA 9.

PORTANTO O SISTEMA:

$x^3 \equiv x \pmod{3}$

$x^3 \equiv x \pmod{p}$

TEM 9 SOLUÇÕES PELO TEOREMA CHINÊS DO RESTO $\longrightarrow$ LOGO $x^3 \equiv x \pmod{3p}$ TEM 9 RESULTADOS.

(7) PORQUÊ $e = 2$ NUNCA DEVERIA SER USADO COMO CHAVE PÚBLICA?

RESOLUÇÃO:

A SEGURANÇA DA CRIPTOGRAFIA RSA SE BASEIA NA IDEIA DE QUE OS NÚMEROS USADOS COMO CHAVE SEJAM TÃO GRANDES QUE SEJA EXTREMAMENTE DEMORADO OU ATÉ MESMO IMPOSSÍVEL DESCRIPTOGRAFAR. PORÉM A CHAVE $e = 2$ REPRESENTA O MENOR NÚMERO POSSÍVEL PARA SER ESCOLHIDO COMO CHAVE. SÓ QUANTO MENOR A CHAVE, MENOR A SEGURANÇA E MAIOR A CHANCE DE DESCRIPTOGRAFAR A MENSAGEM. ENTÃO ESSE VALOR TORNARIA A CIFRA INEFICIENTE, O QUE É DESACONSELHÁVEL.

(8) a) DADOS: p E q PRIMOS; $m = pq$ E $\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases}$

PROVE QUE A ÚNICA SOLUÇÃO EM MÓDULO m É:

$x \equiv (aqq') + (bpp')$. PROVE:

$\longrightarrow$ PRÓXIMA PÁGINA

RESOLUÇÃO:

É POSSÍVEL PROVAR A AFIRMAÇÃO ACIMA MONTANDO O ALGORITMO CHINÊS DO RESTO PARA O SISTEMA NO FORMATO DE UMA TABELA:

	Z_x	M	$\bar{M}$	$\bar{M}^{1}$	$Z \cdot M \cdot \bar{M}^{-1}$
$x \equiv a \bmod p$	a	q	$1/q'$	q'	$a \cdot q \cdot q'$
$x \equiv b \bmod q$	b	p	$1/p'$	p'	$b \cdot p \cdot p'$ +
			CLASSE DE EQUIVALÊNCIA	CLASSE INVERSA	$(aqq') + (bpp')$

↳ A AFIRMAÇÃO ANTERIOR É VERDADEIRA E O SISTEMA TEM SÓ UMA SOLUÇÃO DADA EM: $x \equiv (aqq') + (bpp') \pmod{pq}$.

b) DADOS: $p_1, p_2, \dots, p_m$ PRIMOS ENTRE SI; $MDC(p_i, p_j) = 1$ PARA TODO $1 \leq i < j \leq m$; $m = \prod_{i=1}^{k} p_i$ E
$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \vdots \\ x \equiv a_k \pmod{p_k} \end{cases}$$
PROVE QUE PARA QUAISQUER INTEIROS $a_1, a_2, \dots, a_k$, O SISTEMA POSSUI UMA ÚNICA SOLUÇÃO MÓDULO M, E ESTA SOLUÇÃO É DADA $x = \sum_{i=1}^{k} (a_i q_i q_i')$, ONDE PARA CADA i COM $1 \leq i \leq m$ TEM $q_i = \frac{N}{p_i} = \prod_{\substack{j \in \{1,2,\dots,k\} \\ j \neq i}} p_j$ E q_i' É INVERSO DE q_i E MOD p_i.

RESOLUÇÃO

	a_i	q_i	$\bar{q}_i$	$\bar{q}_i^{1}$	$a_i \cdot q_i \cdot q_i'$
$x \equiv a_1 \pmod{p_1}$	a_1	q_1	$1/q_1'$	q_1'	$a_1 q_1 q_1'$
$x \equiv a_2 \pmod{p_2}$	a_2	q_2	$1/q_2'$	q_2'	$a_2 q_2 q_2'$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$x \equiv a_k \pmod{p_k}$	a_i	q_i	$1/q_k'$	q_k'	$a_i \cdot q_i q_i'$ +

↳ A AFIRMAÇÃO DO ENUNCIADO É VERDADEIRA E O SISTEMA TEM SÓ UMA ÚNICA SOLUÇÃO MOD M USANDO O TEOREMA CHINÊS DO RESTO E AS CONDIÇÕES APRESENTADAS. O RESULTADO FICA O SOMATÓRIO:

$$x = \sum_{i=1}^{k} (a_i q_i q_i')$$

$$x \equiv (a_1 q_1 q_1') + (a_2 q_2 q_2') + \dots + (a_i q_i q_i')$$

EM QUE:

$$q_1 = m/p_1 = \prod_{j \neq 1} p_j$$

$$q_2 = m/p_2 = \prod_{j \neq 2} p_j$$

$$\vdots$$

$$q_i = m/p_i = \prod_{j \neq i} p_j$$

(9) SABEMOS QUE PARA DECODIFICAR UMA MENSAGEM PRECISAMOS DE M E UM NUMERO d QUE É O INVERSO DE e EM $\mathbb{Z}\phi(M)$. O PAR (M, d) É A CHAVE PRIVADA. O MÉTODO DE DECODIFICAÇÃO PELO TEOREMA CHINÊS DO RESTO CONSISTE NUMA MODIFICAÇÃO DA CHAVE PRIVADA DO RSA. UTILIZANDO OS VALORES CALCULADOS.

A CHAVE PRIVADA FICA (p, q, d_p, d_q, q^{-1}) ONDE:

$d_p = d \text{ MOD } (p-1)$; $d_q = d \text{ MOD } (q-1)$; $q^{-1} : q^{-1} \text{ MOD } p$

PARA DECIFRAR UMA MENSAGEM M USANDO O TCR DEVEMOS CALCULAR:

$M_p = c^{d_p} \text{ MOD } p$

$M_q = c^{d_q} \text{ MOD } q$

$M = ((M_p - M_q) q^{-1} \text{ MOD } p) q + M_q$

ESSE MÉTODO É 4 VEZES MAIS RAPIDO DO QUE APLICAÇÃO NORMAL.

(10) DADOS: $(m, e) = (7597, 4947)$ $\phi = 7420$

$(m, d) = (7597, d)$

NECESSARIO ENCONTRAR O d

$ed \equiv 1 \text{ MOD } \phi$

$4947d \equiv 1 \text{ MOD } 7420$

EUCLIDIANO ESTENDIDO PARA $d \rightarrow$

$ed - \varphi(m) r = 1$

$4947d - 7420r = 1$

$d = 3$ $r = 2$

RESTO	QUOCIENTE	X	Y
4947	*	1	0
7420	*	0	1
4943	0	1	0
2473	1	-1	1
1	2	3	-2

ACHADO $d = 3$ CONSTRUIMOS A REGRA DE DECODIFICAÇAO PARA PODEMOS DESCRIPTAR A MENSAGEM.

MENSAGEM: 6803 - 205 - 1126 - 1421 - 1658

REGRA $\rightarrow D(m) = m^3 \equiv b \text{ MOD } 7597$

DIVIDINDO A MENSAGEM EM BLOCOS

$D(6803) = 6803^3 \equiv 146 \text{ MOD } 7597$

$D(205) = 205^2 \equiv 127 \text{ MOD } 7597$

$D(1126) = 1126^2 \equiv 136 \text{ MOD } 7597$

$D(1421) = 1421^2 \equiv 143 \text{ MOD } 7597$

$D(1658) = 1658? \equiv 147 \text{ MOD } 7597$

MENSAGEM DECODIFICADA: 146 - 127 - 136 - 143 - 147

MENSAGEM TRADUZIDA: R - A - I - O - S

(11) PARA ENCONTRAR p E q TENDO COMO DADOS APENAS: m, e E d.
É BASTANTE SIMPLES, BASTA CONTRUIR UM SISTEMA DE EQUAÇÕES, ONDE:

$$\begin{cases} m = p\,q \\ \phi = (p-1)(q-1) \end{cases}$$

SO QUE NÃO TEMOS ϕ MAS TEMOS d E SABEMOS QUE ELE É O INVERSO DE e EM MODULO ϕ, DADO COMO:

$$e d \equiv 1 \bmod \phi$$

RESOLVENDO A EQUAÇÃO MODULAR ACHAMOS ϕ E PODEMOS SUBSTITUÍ-LO NO SISTEMA ACIMA.
RESOLVENDO O SISTEMA, OBTEMOS UM SEGUNDO SISTEMA QUE O SEGUINTE:

$$\begin{cases} m = p \cdot q \\ m = p + q \end{cases}$$

$\rightarrow$ SENDO ESSA EQUAÇÃO O RESULTADO DO PRIMEIRO SISTEMA.

RESOLVENDO O SEGUNDO SISTEMA OBTEMOS OS VALORES DE p E q SEPARADAMENTE.

(12) TRÊS PARES (m, e) DE CHAVE PUBLICAS QUE FORAM GERADAS USANDO SOMENTE 5 PRIMOS. CONSEGUE QUEBRAR PELO MENOS UMA DAS 3 CHAVES?

RESULTADO:

- PARA QUEBRAR UMA CHAVE PUBLICA É NECESSÁRIO ACHAVE PRIVADA, QUE É UM PROBLEMA COMPUTACIONAL.

TEMOS (m, e) MAS COMO ACHAR d

- PARA CALCULAR d PODEMOS APLICAR O ALGORITMO DE EUCLIDES ESTENDIDO A e E $\phi(m) = (p-1)(q-1)$, MAS PARA ACHAR $\phi(m)$ TEMOS QUE TER OS VALORES DE p E q OU SIMPLESMENTE FATORAR m.
  - E A SEGURANÇA DO RSA SE BASEIA JUSTAMENTE NISSO, NA DIFICULDADE DE SE CHEGAR A d CONHECENDO SÓ m E e, PORQUE NO FIM PARA CHEGAR d INEVITAVELMENTE PRECISAMOS FATORAR m, TODAVIA SE m FOR MUITO GRANDE É UM PROBLEMA DADO O FATO QUE NÃO EXISTEM ALGORITMOS RAPIDOS E CONFIAVEIS PARA REALIZAR SUA FATORAÇÃO
- OU SEJA NÃO DÁ PARA QUEBRAR ALGUMA DESSAS 3 CHAVES SABENDO SÓ (m, e) COM m SENDO UM ALGORITMO MUITO GRANDE.