Cifra de César - Princípios de criptografia como trote educacional e em comemoração ao dia da mulher

Rosiane de Freitas[4], Karla Pereira[3,4], Larissa Pessoa[2,4], Ariel Bentes[2,4], Ingrid Santos[1,4], Isabelly Oliveira[1,4] e Tanara Lauschner[4]
[1]Bacharelado em Ciência da Computação
[2]Bacharelado em Engenharia da Computação
[3]Programa de Pós-Graduação em Informática
[4]Instituto de Computação – Universidade Federal do Amazonas (UFAM)
{rosiane, karla.pereira, lsp, alpb, ils, irbo, tanara}@icomp.ufam.edu.br

***Resumo*—Este artigo descreve a aplicação de uma dinâmica sobre os princípios da criptografia chamado a Cifra de César para alunos dos cursos de graduação em Ciência da Computação, Engenharia de Software e Engenharia de Computação na primeira semana de classe como uma forma de integração entre os alunos iniciantes e também em comemoração ao Dia Internacional da Mulher. O objetivo deste trabalho é relatar atividades desenvolvidas e fazer considerações sobre a adequação da proposta, como ela foi recebida e percebida, e a participação das meninas no contexto construído.**

***Abstract*—This paper describes the application of a dynamic about principles of cryptographic called the Caesar Cipher to students of the undergraduate courses in Computer Science, Software Engineering and Computer Engineering in the first week of class as a form of integration between the beginning students and also in commemoration of the International Women's Day. The objective of this paper is to report activities developed and to do considerations about the adequacy of the proposal, how it was received and perceived, and the girls' participation in the context constructed.**

***Index Terms*—IEEE, IEEEtran, journal, LaTeX, paper, template.**

I. Introdução

Todo início de ano letivo, alunos que ingressam pela primeira vez nos cursos de graduação (popularmente conhecidos como calouros), chegam em um novo ambiente de ensino bem diferente do que estavam acostumados no colegial e em geral, demonstram-se deslocados, não conhecendo a estrutura e funcionamento do curso universitário e nem tampouco os colegas de sua turma e de outros cursos. Passar no vestibular, além de vários sentimentos e novidades na vida do estudante, também implica passar por um ritual chamado "trote".

O trote é um rito de iniciação que remonta à Idade Média e designa os atos de zombaria e a imposição de tarefas a que veteranos sujeitam aos calouros. Trata-se de ritual de iniciação às avessas, porque perpetra a violência e o desrespeito às leis. O trote teve início na Europa e lá foi marcado pela violência desmedida. No Brasil, foi introduzido no século XVIII, por influência de estudantes da Universidade de Coimbra. Em 1831, em Recife, ocorreu a primeira morte oriunda de trote, seguida de várias outras tragédias [10].

Seu caráter violento e humilhante não impediu que se tornasse uma tradição em várias universidades brasileiras. Justificada pelos alunos de que deve ser mantida, pois tem como objetivo a integração dos novos alunos.

Em um estudo de caso realizado na Universidade Federal de São Carlos sobre a recepção de calouras no curso de Psicologia pôde se observar dois pontos importantes. O primeiro remete ao fato de que muitas calouras concordaram em participar do trote pois sentiram a importância destas brincadeiras "saudáveis" para marcar o sucesso de terem sido aprovadas no vestibular, mesmo que às custas de uma humilhação coletiva. O segundo fato refere-se ao depoimento de uma novata que, ao ser questionada se a realização dos trotes facilitou a integração entre caloura e veterana, asseverou: "Sim, foi fundamental. Quem não participou ficou um pouco deslocado depois" [12]. Assim, podemos perceber que de um lado temos o anseio de comemoração pela aprovação no vestibular e de outro a preocupação de se sentir aceito no novo meio acadêmico. Esses dois pontos alinhados com a aceitação dos agentes educacionais permitem a perpetuação de trotes contendo violência física e psicológica, ainda que não aparentes em um primeiro momento.

Com a má fama dos trotes, alunos veteranos foram estimulados a buscar outras formas de interagir com esses novos ingressantes, propondo o que ficou conhecido como "trote solidário", onde suas práticas passaram a ser benéficas e de cunho social, como: doar sangue, plantar árvores, interagir com crianças ou idosos em instituições e arrecadar alimentos [11].

Um grande exemplo de trote, sem violência ou humilhação, é a recepção aos calouros do curso de pedagogia realizada na Universidade de Brasília. A atividade nasceu a partir da necessidade concreta dos próprios estudantes de criar espaços de discussão e formação política dos estudantes que ingressavam no curso, tornando os temas e espaços mais familiares e qualificando as falas a partir do debate de ideias. Isso faz

com que a motivação para a realização das atividades esteja na sua própria execução, tornando o espaço desejado pelos seus participantes. Temas pouco tratados na universidade, e de importância ímpar na sociedade, tem seu espaço de aprofundamento, crítica, e ação na Recepção aos Calouros. Desses temas podemos citar o próprio trote tradicional, uma vez que é inerente a ele um sistema de opressão, pois parte da hierarquização dos conhecimentos [13].

Outro exemplo interessante de trote amigável foi a atividade realizada pelo Projeto #Include $< meninas.uff >$ na Universidade Federal Fluminense (UFF) com os calouros da turma de Ciência da Computação. Na atividade, foi possível observar a interação dos calouros através de dinâmicas de apresentação e promover o debate a respeito do baixo número de meninas no curso, abrindo espaço para elas se expressarem [14].

Dado esse contexto, neste ano, particularmente, a primeira semana de aula na referida Instituição de Ensino Superior (IES) onde ocorreu o foco do estudo, aconteceu no começo do mês de março, incluindo a data 08 de março.

O dia 08 de março, foi oficializado pela Organização das Nações Unidas (ONU) em 1975 como "Dia Internacional da Mulher", para celebrar conquistas políticas e sociais femininas. Essa homenagem, é devido às mulheres que trabalhavam nas fábricas nos EUA e em alguns países da Europa, que iniciaram uma campanha dentro do movimento socialista que buscavam direitos igualitários e reivindicaram as condições de trabalho, pois eram ainda piores que homens na época [16].

Sendo assim, diante da necessidade de realizar uma recepção aos calouros, possibilitando essa integração entre a própria turma em conjunto com outras turmas de Computação da referida unidade de ensino, foi planejada uma atividade para também aproveitar a comemoração do dia internacional da mulher, através de uma dinâmica envolvendo princípios da criptografia, onde alunas receberam as cegas o papel inicial de liderança dos grupos, e as frases em uso tiveram motivação para a discussão de gênero.

O objetivo deste artigo é apresentar a dinâmica realizada e tecer considerações sobre a adequabilidade da proposta, como foi recebida e percebida, e a participação das meninas diante do contexto construído a partir das atividades propostas.

Este trabalho está organizado da seguinte maneira: a Seção 2 aborda a história, teoria e aplicações da Cifra de César, a Seção 3 descreve a proposta de dinâmica aplicada nos três cursos de graduação, a Seção 4 relata a análise dos resultados, a Seção 5 apresenta as considerações finais. E, por fim, as referências que embasam este documento são listadas.

II. Cifra de César

Criptografia é o nome dado ao processo de converter texto claro, isto é o texto que é inteligível, em texto cifrado. O termo criptografia é derivado das palavras gregas *"kryptós"*, que significa "esconder" e *"gráphein"*, que significa "escrever". Dessa forma, o significado do termo criptografia é melhor parafraseado como "escrita oculta".

A criptografia é uma ciência matemática que trata da conversão de textos claros (texto comum, não criptografado) em textos ininteligíveis (texto criptografado), com o objetivo de ocultar seu conteúdo semântico, assim dificultando alterações não detectadas, e uso não autorizado. Se o processo de conversão for reversível, temos então a restauração dos dados criptografados, tornando-os inteligíveis. Consequentemente, a criptografia refere-se ao processo de proteção de dados em um sentido amplo [6].

A criptografia provavelmente é o aspecto mais importante da segurança de comunicações e está se tornando cada vez mais importante como um componente básico para a segurança do computador [4]. A criptografia é uma arte antiga e, de certa forma, há pouco tempo a definição acima teria sido bastante adequada. Contudo, nos últimos trinta anos, expandiu-se para abranger muito mais do que mensagens secretas ou cifras. Por exemplo, protocolos criptográficos para provar a sua identidade online com segurança (como nos sites de banco) ou assinar contratos digitais vinculativos agora são ao menos tão importantes quanto as cifras [5].

As técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário, é claro, deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados. Existem duas técnicas de criptografia que foram utilizadas ainda na antiguidade, sendo elas a de transposição e a de substituição.

Na transposição, as letras de uma mensagem são rearranjadas de maneira simples, gerando um anagrama. Para que a transposição seja eficaz, o arranjo de letras precisa seguir um sistema simples, que tenha sido acordado previamente entre o remetente e destinatário, e também mantido em segredo de intrusos.

Já a substituição é uma alternativa a transposição, esta técnica consiste em agrupar as letras do alfabeto randomicamente, e assim substituir cada letra na mensagem de texto aberto pelo seu par. Essa forma de escrita secreta é chamada de cifra de substituição, pois cada letra do texto aberto é substituído por uma letra diferente, assim atuando de maneira complementar a cifra de transposição. Na transposição cada letra mantém sua identidade, mas muda de posição, enquanto que na substituição cada letra muda sua identidade e mantém sua posição.

O primeiro uso da cifra de substituição com propósito militar que se tem conhecimento aconteceu nas Guerras da Gália de Júlio César. O imperador romano Júlio César descreveu como enviou uma mensagem a Cícero, que estava cercado e a beira da rendição. A substituição foi feita de forma a substituir as letras romanas por letras gregas, tornando a mensagem ininteligível para o inimigo, a forma de substituição empregada por Júlio César ficou conhecida como cifra de César [15].

A cifra de César funciona tomando cada letra da mensagem de texto aberto e substituindo-a pela k-ésima letra sucessiva do alfabeto, permitindo a rotatividade do alfabeto, isto é, a letra *Z* seria seguida novamente da letra *A*. Por exemplo, se $k = 4$, então a letra *A* do texto claro fica sendo *E* no texto cifrado; *B* no texto claro se transforma em *F* no texto cifrado, e assim por diante, como apresentado na Figura 2. Embora

o texto cifrado de verdade pareça não ter nexo, não levaria muito tempo para quebrar o código se soubesse que foi usado a cifra de César, pois há somente 25 valores possíveis para as chaves. O deslocamento do alfabeto na Cifra de César com chave igual a 3, seria dado conforme a figura 1.

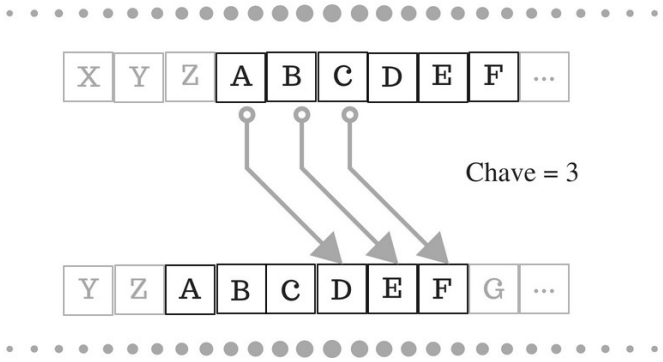

Figura 1. Demonstração do deslocamento com chave igual a 3.

A equação da criptografia de César é dada por (1), onde *C* é o texto cifrado, *k* é a chave de deslocamento e *n* é o texto claro. O operador **mod** é o resto da divisão por 26, que é a quantidade de letras do nosso alfabeto.

$$C = (k + n) mod 26 \quad (1)$$

A equação da descriptografia de César é dada por (2), onde *D* é o texto cifrado, *k* é a chave de deslocamento e *n* é o texto claro.

$$D = (k - n) mod 26 \quad (2)$$

Aplicando a cifra de César, com a chave de deslocamento *k = 2*, para criptografar a mensagem ADA LOVELACE, obtemos a correlação entre o alfabeto claro e o alfabeto cifrado, conforme apresentado na Figura 4, com um deslocamento de 2 posições, de tal forma que a mensagem criptografada seja CFC NQXGNCEG.

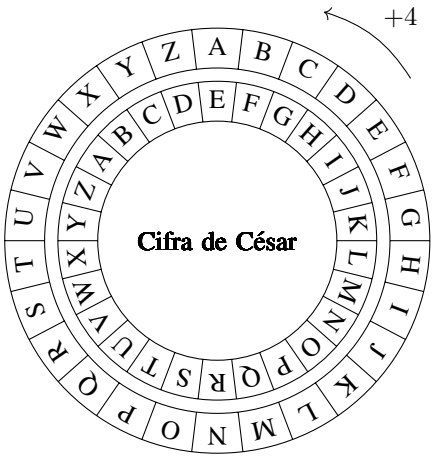

Figura 2. O disco cifrado de César é usado para mostrar como as letras do alfabeto aberto (disco mais externo) estão relacionadas com as letras do alfabeto cifrado (disco mais interno), onde dada uma chave de deslocamento *k*, movimenta-se o disco mais interno em sentido anti-horário *k* vezes.

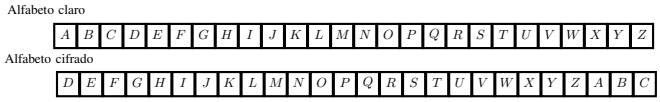

Figura 3. Cifra de César representada em vetores, onde o vetor superior representa o alfabeto claro, e o vetor inferior representa o alfabeto cifrado. Este exemplo está com uma troca de três posições, onde o *A* torna-se o *D*, o *B* torna-se o *E*, e assim por diante.

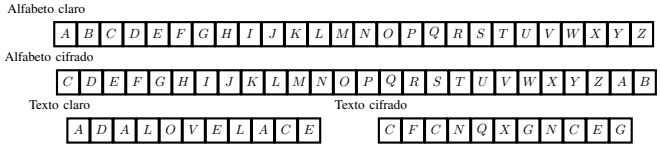

Figura 4. Cifra de César representada em vetores, onde o vetor superior representa o alfabeto claro, e o vetor inferior representa o alfabeto cifrado. Este exemplo está com uma troca de duas posições, que aplicado ao o texto claro "ADA LOVELACE" assume a forma do texto cifrado " CFC NQXGNCEG".

A cifra de César é um tipo de cifra monoalfabética, que também substitui uma letra do alfabeto por outra. Contudo, na cifra monoalfabética qualquer letra pode ser substituída por qualquer outra, contanto que cada letra tenha uma única substituta e vice-versa, em vez de fazer isso seguindo um padrão regular, como na cifra de César. A cifra monoalfabética também parece ser melhor que a cifra de César, pois há 26! (da ordem de 10^{26}) possíveis pares de letras, em vez de 25 pares possíveis [7].

Um caso especial da cifra de César é a cifra de ROT-13, aplicada aproximadamente em 1980 na USENET, era utilizada para ocultar piadas politicamente incorretas, ou spoilers. Nela aplica apenas aos caracteres alfabéticos da língua inglesa e com um deslocamento de 13 posições, ou seja, é a criptografia de uma mensagem trocando cada uma das letras na primeira metade do alfabeto com a letra correspondente na segunda metade do alfabeto, isto é, realiza-se um deslocamento de 13 posições. Assim, *A* torna-se *N*, *B* torna-se *O*, e assim por diante e, inversamente *N* torna-se *A*, *O* torna-se *B*, e assim por diante. Números, espaços e pontuação não são alterados. É usada principalmente para proteger endereços de correio eletrônico, e também mensagens postadas em grupos e listas de discussão online [22].

E uma variação da cifra de César é a cifra de Vigenère, que é uma cifra do tipo substituição polialfabética e consiste em utilizar diferentes regras monoalfabéticas enquanto se prossegue pela mensagem de texto claro. A substituição polialfabética é caracterizada por utilizar um conjunto de regras de substituição monoalfabética que consiste nas 26 cifras de César, com deslocamento de 0 a 25. Cada cifra é indicada por uma letra-chave, que é a letra do texto cifrado que substitui a letra do texto claro, inteligível. Assim, uma cifra de César com deslocamento d é indicada pelo valor de chave *k*. Dessa forma, ele estaria mudando o modo de embaralhamento durante a cifragem, conhecido como substituição polialfabética, e tornaria a cifra difícil de ser quebrada [17].

Informações	Cifra de César	Cifra de ROT13	Cifra de Vigenère
Origem	Usada pelo imperador romano Júlio César em 50 a.C.	Aplicada na USENET aproximadamente em 1980	Inventada em 1586, por Blaise de Vigenère
Classe	Substituição simples	Substituição simples de 13 posições	Substituição com palavra-chave
Tipo	Monoalfabética, pois usa apenas um alfabeto cifrante, e monogrâmica, pois trata cada um dos caracteres individualmente	Monoalfabética, pois usa apenas um alfabeto cifrante, e monogrâmica, pois trata cada um dos caracteres individualmente	Polialfabética, pois usa vários alfabetos cifrantes, e monogrâmica, pois trata cada um dos caracteres individualmente
Nível de segurança	Baixissíma	Baixa	Baixa
Uso	Aplicável apenas em textos curtos	Aplicável apenas aos caracteres alfabéticos da língua inglesa	Aplicável em textos longos e curtos
Criptoanálise	Uma simples criptoanálise baseada na característica estatística da língua é suficiente para decifrar o texto	Uma simples criptoanálise baseada na característica estatística da língua é suficiente para decifrar o texto	Uma simples criptoanálise baseada na característica estatística da língua é suficiente para decifrar o texto

Tabela I
ANÁLISE COMPARATIVA ENTRE A CIFRA DE CÉSAR, CIFRA DE ROT-13 E CIFRA DE VIGENÈRE.

III. DINÂMICA

Esta seção descreve a Dinâmica baseada na Cifra de César [3], aplicada pela primeira vez em cursos da área de Computação na Universidade Federal do Amazonas (UFAM), com o objetivo de observar o comportamento dos alunos recém-matriculados além de recepcioná-los de forma positiva em seus primeiros dias de aula. Também descreve os três cursos de graduação na área de computação oferecidos pela UFAM - que são Ciência da Computação, Engenharia da Computação, Engenharia de Software-, o planejamento da dinâmica para ser aplicada ao contexto de alunos recém-matriculados da UFAM, a descrição de quais materiais e como eles foram produzidos e usados na dinâmica, e como foi realizada a aplicação da dinâmica no dia internacional das Mulheres.

A. Sobre os cursos de graduação em Computação selecionados

Os cursos da área de Computação da UFAM são divididos em dois turnos. No turno diurno (manhã e tarde) são ofertados Ciência da Computação e Engenharia de Computação, no turno noturno (tarde e noite) Engenharia de Software, foi considerado que o curso de Sistemas de Informação tornou-se o curso de Engenharia de Software em 2018. Nesse ano de 2018, foram matriculados 145 novos alunos, desse total apenas 25 são mulheres, representando apenas 18% do total.

Nos cursos diurnos foram matriculados 52 alunos em cada um, destes 4 (7%) são mulheres em Engenharia da Computação e 11 (21%) são mulheres em Ciência da Computação. Já no curso noturno, Engenharia de Software, foram matriculados 41 novos alunos, destes 10 (24%) são mulheres. A análise foi realizada através de dados obtidos com a Coordenação Acadêmica da UFAM. É possível observar essa distribuição de forma gráfica na figura 5.

Ao comparar a quantidade de alunas recém-matriculadas em 2018 com a de anos anteriores [23] é possível perceber que houve uma redução mínima na quantidade total de recém-matriculadas em três cursos. A partir da análise do comparativo anual de quantidade de alunas matriculadas por curso [24], pode se concluir que em Ciência da Computação e Engenharia de Software se manteve a mesma porcentagem de alunas ingressantes na turma enquanto que houve uma redução mínima em Engenharia da Computação em relação ao anos anteriores. Vale ressaltar que a turma de Engenharia de Software em 2018 faz parte da continuação ao acompanhamento de ingressantes iniciado na turma de Sistema de Informação.

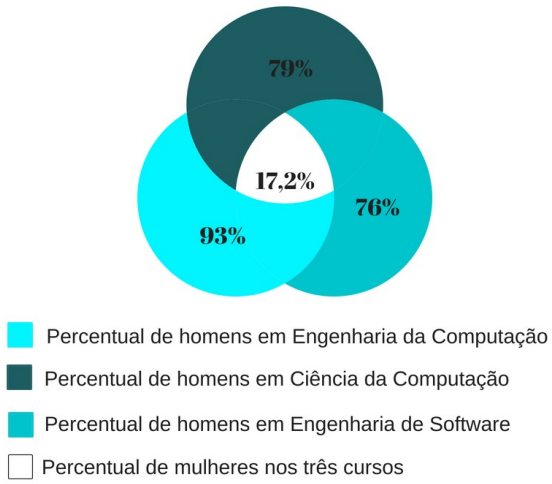

Figura 5. Distribuição das turmas selecionadas por gênero

B. Sobre a metodologia da dinâmica

A metodologia da dinâmica da cifra de césar [3] foi adaptada para o contexto em que fosse possível envolver mais de um curso durante sua execução. Ao todo, participaram como observadores da execução 15 membros do Projeto de Extensão Cunhantã Digital: duas professoras, 1 aluna de doutorado e 12 alunos de graduação.

Inicialmente ao solicitarmos a participação das turmas foi informado apenas que seria uma ação de boas vindas ao alunos recém-matriculados, além de aproveitar a data do dia internacional da mulher para apresentar o projeto de incentivo e empoderamento de mulheres na TI presente na Instituição.

Como a dinâmica foi aplicada para mais de um curso e as turmas tem aula em turnos diferentes percebeu-se a necessidade de aplicar duas vezes a dinâmica no dia escolhido. Então, a dinâmica ocorreu em dois turnos: matutino com a previsão de 104 alunos, destes 15 eram mulheres; e noturno com previsão de 41 alunos, destes 11 eram mulheres.

Baseado no turno com o maior número de participantes previstos para a dinâmica, foi planejado para que em qualquer turno houvesse no máximo 20 equipes a fim de garantir que na maior quantidade de grupos houvesse uma menina e que os grupos não tivessem integrantes demais ociosos por serem numerosos. Com isso, ficaria possível reutilizar o material para outras aplicações.

Em um primeiro momento (se houver mais de uma turma então devem ser trabalhadas separadamente em cada sala) uma professora do projeto apresentou o Cunhantã Digital e deu as boas vindas ao calouros, em seguida, foi solicitado que:

- Para os alunos recém-matriculados, cada aluno apresentasse o seu colega ao lado para a turma.
- Para os membros do projeto, observasse o comportamento dos alunos ao descreverem seu colega de classe;

Por último, foi iniciada a dinâmica da Cifra de César dentro de Sala com os seguintes passos:

- entregar um número de uma sequência para cada uma das meninas na turma;
- distribuir outros números restante da mesma sequência para os meninos, fazendo com que equipes fossem formadas com os colegas que tivessem o número igual;

Se houver mais de uma turma então elas devem ser juntadas para que a formação final das equipes sejam formalizadas. Por fim, foi concedido a cada grupo um copo decodificador e uma placa contendo o mesmo conjunto de frases codificadas para estabelecer o nivelamento. Aos poucos algumas dicas foram reveladas a fim de facilitar a resolução das frases codificadas da dinâmica.

C. Sobre o planejamento e confecção do material

A equipe do projeto foi dividida em grupos para participar da execução no dia da dinâmica e para confeccionar o material. Também existiram integrantes que participaram simultaneamente nos dois grupos, com isso foi possível reduzir as dúvidas quanto ao planejamento durante a execução.

Para a confecção do material para 20 equipes foi necessário:

- 8 cartelas numeradas de 1 a 20 feitas de papel cartão (figura6 a)). para formar equipes com oito pessoas no máximo, uma dessas cartelas foi feito em tamanho A4 e os restantes em tamanho A7;
- 40 (quarenta) copos de plástico grande (500 ml);
- 40 (quarenta) fitas de papel com o alfabeto completo impresso de forma semelhante a uma fita métrica e no tamanho da circunferência da borda superior de um copo (figura 6 b)).
- fita adesiva para colar cada fita em cada borda superior dos copos (figura 6 b));
- Conjuntos de mensagens a serem criptografadas. Foram utilizadas as seguintes mensagens de empoderamento:

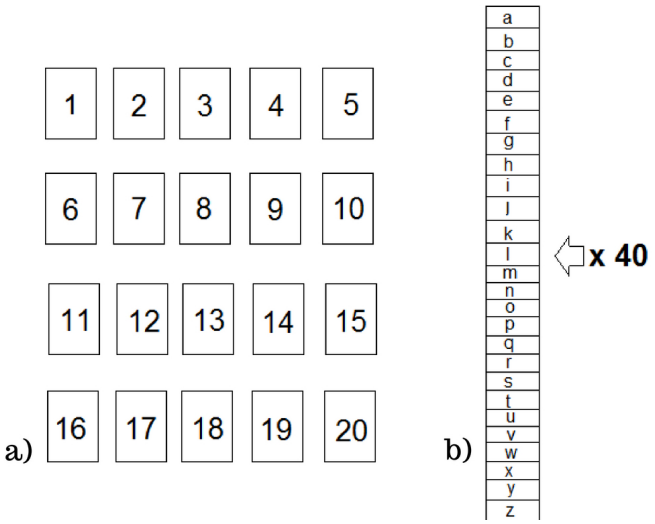

Figura 6. a) Cartelas enumeradas que são entregue aos alunos. b) Representação das fitas alfabéticas

” Mulher na computação não é um bug ”;
“Não é não, depois do não é tudo assédio”;
” Respeita as cunhantãs”;
” Aprender a programar e evitar que você seja programado”;
” Lugar de mulher é onde ela quiser”.

- 20 (vinte) placas feitas de papel cartão com o conjunto de frases criptografadas como no exemplo a seguir:
  Considere n = 12
  1 - *Ygxtqd zm oyabgfmoma zma q gy ngs.*
  2 - *Zma q zma. Pqbaue pa zma q fgpa meeqpua.*
  3 - *Dqebqufm me ogztmzfme.*
  4 - *Mbdqzpqd m bdasdmymd q qhufmd cgq haoq eqvm bdasdmympa.*
  5 - *Xgsmd pq ygxtqd q azpq qxm cgueqd.*

- 20 (vinte) placas feitas de papel cartão para a dica da fórmula matemática (3).

$$E\{n\}(x) = \frac{(x+n)}{mod 26} \tag{3}$$

Essa placa continha a dica apresentada com o seguinte conteúdo:

Primeira dica: Fórmula matemática
26 = constante representando o tamanho do alfabeto, numerado de 0 a 25, onde A = 0 e Z= 25;
x = letra a ser criptografada (trocada) por outra;
n = número de trocas
Ex.: E{3}(A) = (A + 3)/mod 26
*E{3}(A) = (*0 + 3*)/mod* 26
E{3}(A) = 3
Então, se n= 3 *e x = A, A deve ser trocado por D.*
Os decodificadores foram feitos da seguinte maneira: Na borda

superior de cada um (figura 7 a)) dos 40 copos foi colada uma fita de alfabeto.

Para cada decodificador foram necessários dois copos e duas fitas de alfabeto. Por fim o decodificador é formado por esses dois copos encaixados um dentro do outro, formando um codificador/decodificador de César (figura 7 b));

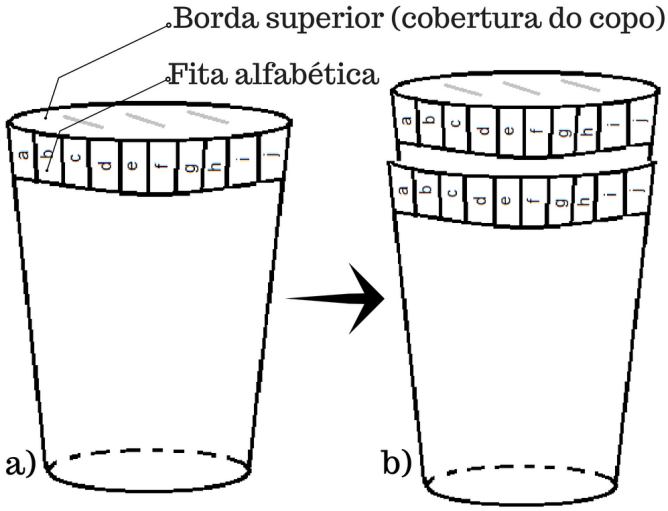

Figura 7. a) Peça de um Decodificador da Cifra de César. b) Representação dos Codificadores/Decodificadores confeccionados para a dinâmica

Com os 40 (quarenta) copos foi possível confeccionar 20 (vinte) decodificadores (figura 8), 1 (um) para cada equipe.

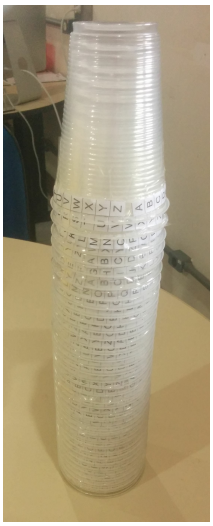

Figura 8. 20 Codificadores/Decodificadores confeccionados para a dinâmica

D. Aplicação da dinâmica para alunos de graduação

A aplicação da dinâmica foi feita no dia internacional da Mulher (8 de Março de 2018) para 104, sendo 52 alunos de Ciência da Computação e 52 alunos de Engenharia da Computação no período da manhã e no período da noite para 41 alunos de Engenharia de Software.

A dinâmica ocorreu em dois níveis tanto no turno da manhã quanto da noite. Inicialmente no turno da manhã, em um primeiro nível, as turmas de Ciência da Computação e Engenharia da Computação foram trabalhadas separadamente representadas na figura 9 a seguir.

Figura 9. Representação das turmas trabalhadas separadamente

Em cada sala, foi solicitado que os próprios alunos se apresentassem. No entanto, ao invés de cada aluno se apresentar, o mesmo teria que apresentar o colega ao lado, como por exemplo na figura 10. Dessa maneira foi possível observar o comportamento dos alunos descrevendo uns aos outros e também os critérios usados na descrição, dentre critérios físicos ou comportamentais.

Figura 10. Alunos apresentando seus colegas no primeiro nível da dinâmica

Em seguida, entregou-se um número diferente de uma sequência para todas as alunas da turma. Para todos os meninos, distribuiu-se aleatoriamente números da mesma sequência anterior para formarem grupos de um determinado número recebido, de tal forma que todos os meninos tivessem que procurar a menina com o número correspondente. Assim permitindo que os grupos tivessem ao menos uma mulher.

Mas a formação final dos grupos foi feita em um segundo nível, pois ao entregar o número para os alunos e alunas garantiu-se que os números da sequência estivessem misturados entre as duas turmas. Então ao juntar as turmas de Engenharia da Computação e Ciência da Computação os grupos foram formados com alunos das duas turmas (figura 11).

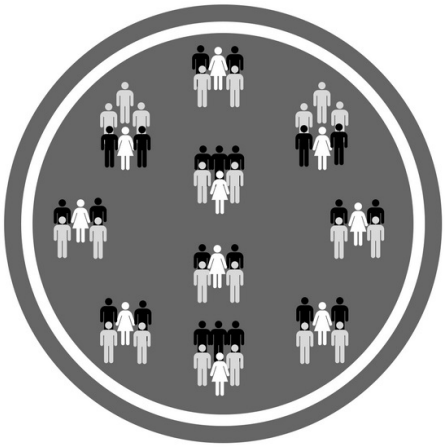

Figura 11. Representação dos grupos formados a partir da junção das turmas de Ciência da Computação e Engenharia da Computação

Então foi entregue a cada equipe um decodificador juntamente com um papel contendo frases codificadas, a missão era decifrá-las (figura 12). Utilizou-se mensagens criptografadas de empoderamento como: ”Mulher na computação não é um bug”, ”Não é não, depois do não é tudo assedio”, ”Aprender a programar e evitar que você seja programado”, ”Respeita as cunhantãs”, ”Lugar de mulher é onde ela quiser”. As mensagens foram criptografadas com base no conceito da Cifra de César, já anteriormente explicado. Entretanto, nada fora dito aos alunos sobre a Cifra de César. O uso de celulares foi proibido para que fosse possível instigar a curiosidade deles em analisar o material que receberam. Assim foi possível analisar quais métodos usariam para desvendar as mensagens.

Figura 12. Turmas de Ciência da Computação e Engenharia da Computação durante a execução da Dinâmica

Também foi possível notar o comportamento organizacional dos meninos e das meninas, a fim de verificar se elas manteriam (ou não) a posição de liderança. Em seguida, dicas foram reveladas por etapas durante a execução da dinâmica. Primeiramente, uma folha contendo a fórmula matemática da criptografia foi entregue a cada grupo. A segunda dica foi informar que era a Cifra de César, a terceira e última dica foi entregar a troca da primeira letra de uma das palavras criptografadas de cada grupo. Por fim, ganhou a equipe que resolveu o maior número de palavras no menor tempo com um número mínimo de dicas.

Em seguida, no turno da noite a mesma dinâmica foi aplicada com apenas a turma de Engenharia de Software (figura 13). A metologia foi seguida porém com apenas uma alteração na quantidade de equipes. Nesta turma foram formadas 10 equipes entre os alunos da própria turma. A adaptação foi a redução da sequência para representar uma quantidade menor de grupos. Foi utilizado o mesmo conjunto de frases criptografadas aplicadas para o turno da manhã a fim de que esta turma também ficasse com a dificuldade nivelada com as outras.

Figura 13. Turmas de Engenharia durante a execução da Dinâmica

IV. Discussão e análise dos resultados

A dinâmica, aplicada pela primeira vez na UFAM, foi realizada na primeira semana de aula do ano letivo de 2018 então os alunos ingressantes pouco conheciam os seus colegas de turma e os colegas de outros períodos de seus cursos. Com exceção de metade da turma de Ciência da Computação, estes já estavam matriculados antes do início do ano letivo, quando realizaram um curso de nivelamento de duas semanas. Nas turmas também haviam grupos pequenos de alunos que vinham da mesma escola de ensino médio. Ainda assim, foi possível perceber durante a primeira semana de aula que muitos se conheciam pouco para fazerem descrições mais profundas de seus colegas.

Com base nas apresentações dos alunos no primeiro nível da dinâmica, percebeu-se as diferenças de descrições por gênero. Os meninos descreveram os colegas de gênero masculino como: ”legal”, ”parece ser inteligente”, ”esse aí sabe programar”. Já a descrição dos meninos para as colegas do gênero feminino se dividia entre quando eles as conheciam: era mencionado sobre o que elas gostavam ou faziam como estudos e hobby; e quando não as conheciam: mencionavam sobre o “cabelo cacheado”, “estatura media”, “cabelo liso”. Observa-se que quando os meninos foram descrever outros meninos, eles destacaram características comportamentais. Quando a descrição passou a ser sobre as meninas, eles identificaram em sua maioria características físicas.

Em seguida, no segundo nível da dinâmica cada grupo tinha uma menina presente e ela quem recebeu a mensagem. Em alguns grupos, elas permaneceram como líderes (na figura

14). Em outros não ficou claro se existia liderança. Em um determinado grupo, o papel com a mensagem saiu rapidamente das mãos femininas.

Figura 14. Grupo resolvendo as frases criptografadas em que nota-se a liderança feminina.

Além de permitir essas observações, a dinâmica introduziu de forma lúdica os princípios de criptografia e iniciou uma breve discussão com os calouros sobre a participação mais efetiva das meninas nos cursos de exatas e principalmente de exercer mais papéis de liderança no mercado de trabalho.

Por fim, pode-se notar que os alunos receberam a proposta de boas vindas de forma positiva visto pelas figuras 15, 16, 17.

Figura 15. Finalização da Dinâmica.

Figura 16. Alunas de Ciência da Computação e Engenharia da Computação ingressantes em 2018.

Figura 17. Alunas de Engenharia de Software ingressantes em 2018.

V. Aplicando uma versão simplificada da dinâmica em uma escola de informática para crianças

A dinâmica sobre a Cifra de César também foi estendida para uma escola de informática da cidade em questão, em evento comemorativo ao mês da mulher, em março. Mães e filhas participaram das atividade, envolvendo alguns funcionários também. No caso, a dinâmica ocorreu ao mesmo tempo com as crianças e mães, mas em equipes separadas. Cada equipe recebeu um "decodificador da Cifra de César" e as 03 (três) palavras a serem cifradas, que foram de personagens femininos (Tecna e Shuri) e históricos (Ada Lovelace). A escolha de palavras apenas, ao invés de frases como na dinâmica principal, ocorreu porque neste caso seriam crianças e suas mães, e não estudantes universitários de cursos de Computação. Assim, foram escolhidas personagens do universo feminino que expressassem uma forte relação com o universo tecnológico computacional (como a Tecna e Shuri) ou um nome histórico famoso, caso da Ada Lovelace.

A personagem Tecna (Figura 18.a) é considerada a fada da tecnologia e faz parte do Clube da Winx, sendo a especialista em ciência nesse grupo [9]. A outra personagem escolhida foi a Shuri (Figura 18.b), irmã caçula do personagem Pantera Negra, história em quadrinhos da editora Marvel Comics e que foi transformado em filme recentemente, lançado com estrondoso sucesso. A Shuri é a responsável por todo o desenvolvimento tecnológico da nação Wakanda, sendo considerada uma mente brilhante, cientista inventora de artefatos tecnológicos [18]. Por fim, a terceira é uma célebre personalidade da nossa história. Ela é considerada a primeira programadora da história, mas que ficou mais conhecida do público geral por ser a filha do Lord Byron, famoso poeta inglês, Augusta Ada Byron, condessa de Lovelace - mais conhecida como "Ada Lovelace"(Figura 18.c) [1] . Ela que em torno de 1840 elaborou o primeiro programa com as anotações sobre a máquina analítica de Babbage. A linguagem Ada foi criada na década de 1970 pelo Departamento de Defesa dos Estados Unidos em homenagem a Ada Lovelace [8].

O impacto na escolha dos nomes femininos foi extremamente positivo, o que indicou que a escolha foi certeira. Sobre a dinâmica, a criança mais nova que recebeu o copo com as Cifras de César tinha 7 anos e apesar de não se intimidar e

Figura 18. Personagens femininas usadas na dinâmica sendo (a) Tecna, personagem do desenho animado do Clube Winx, (b) Shuri, personagem da história do Pantera Negra e (c) Ada Lovelace, primeira programadora da história.

se envolver bastante, sentiu bastante dificuldade nesse jogo de letras e não conseguiu descriptografar as palavras sozinhas, nem recebendo algumas dicas dadas aos outros. Entretanto, quando foram revelados os nomes das personagens da atividade, ela logo associou o nome Tecna com Tecnologia. Uma outra criança com 10 anos, apesar de ter apresentado um pouco de dificuldade, conseguiu descobrir todas as palavras conforme foi recebendo as dicas. No caso das mães, apesar de algumas demonstrarem dificuldade maior do que a das crianças, a maioria conseguiu decifrar mais rapidamente do que a maioria das crianças, após algumas dicas. Deve-se ressaltar que as mães eram em geral jovens, algumas ainda universitárias. Por fim, como já era esperado, os funcionários conseguiram decifrar os nomes das personagens com maior rapidez em relação a todos, conforme iam recebendo algumas dicas. A atividade permitiu integrar crianças, mães e funcionários da escola, que deram um retorno muito positivo em relação à atividade realizada, terminando com uma integração total, muitos agradecimentos, alegrias e fotos para registro.

VI. Considerações Finais

Uma vez que a participação de mulheres nas áreas de Computação e Tecnologia da Informação é extremamente baixa [3], atividades de acolhimento e receptividade são primordiais na integração de novos alunos, principalmente quando a abordagem e em prol do papel que a mulher pode exercer nas áreas de exatas e tecnológicas. A dificuldade de inclusão de mulheres em ambientes dominados por homens é um problema atual [3] e foi percebida na dinâmica quando em alguns grupos as meninas que estavam com a mensagem criptografada deveriam liderar a equipe e tiveram um papel de coadjuvante. Outro ponto a destacar, foram as percepções dos meninos sobre os participantes de ambos os gêneros. Ficou perceptível que, para os meninos, as meninas não apresentavam características de cunho profissional e/ou técnico. Infelizmente, isso ainda e reflexo de uma estereotipagem cultural em relação ao gênero feminino. Como trabalhos futuros, sugere-se aplicar a mesma dinâmica com as meninas recebendo a mensagem criptografada e orientações condicionadas para exercer determinados tipos de papéis na equipe e observar o comportamento dos participantes, independente do gênero.

Referências

[1] ADA Lovelace Biography. (2018). *Biography* [Online]. Available: https://www.biography.com/people/ada-lovelace-20825323. In: April 21 2018.

[2] Buchmann, J. A. (2004). *Introduction to Crypyography*. Springer.

[3] Mochetti, K., Salgado, L., Zerbinato, A. V., Souza, B. L., and Avelino, M. R. E. (2016). *Ciencia da Computacao tambem e coisa de menina!* Instituto de Computacao - Universidade Federal Fluminense(UFF), Rio de Janeiro.

[4] Council, N. R., Committee, S. S. S., et al. (1990). *Computers at risk: safe computing in the information age*. National Academies Press.

[5] Talbot, J. and Welsh, D. (2006). *Complexity and Cryptography: An Introduction*. Cambridge University Press.

[6] Oppliger, R. (2005). *Contemporary Cryptography*. Artech House Publishers.

[7] Kurose, J. F. and Ross, K. W. (2012). *Computer Networking: A Top-Down Approach*. Pearson, 6th Edition.

[8] Lopes, L. (2018). *10 fatos sobre Ada Lovelace que farão você admirá-la ainda mais*. [Online]. Available: https://revistagalileu.globo.com/Sociedade/Curiosidade/noticia/2018/02/10-fatos-sobre-ada-lovelace-que-farao-voce-admira-la-ainda-mais.html. In: 19. abr. 2018.

[9] Martins, A. A. (2011). *Mundinho Encantado dos Seres Mágicos*. [Online]. Available: http://mundinhoencantadodosseresmagicos.blogspot.com.br/2011/11/tecna-fada-da-tecnologia.html. In: April 19 2018.

[10] Camilo, A. (2010). *Do trote universitário como atentado aos direitos da personalidade do acadêmico*. XIX Encontro Nacional do CONPEDI. Anais. Fortaleza.

[11] Mitye, C. (2018). *A nova cara do trote universitário - Mundo Educação*. [Online]. Available: http://mundoeducacao.bol.uol.com.br/educacao/a-nova-cara-trote-universitario.htm. In: April 21 2018.

[12] Zuin, A. A. S. (2002). *O trote no curso de pedagogia e a prazerosa saudação sadomasoquista* In *Educação e Sociedade, Agosto.*

[13] Almeida, G. F., Fonseca, M. P. and Cerveira, R. S. (2011). *Recepção aos Calouros como espaço de convivência e transformação* In *Universidade de Brasília*

[14] Mochett K., Bravo, R., Salgado, L., Leitão, C., Braga, C., Hecksher, G. and Pontes, K. (2017). *Discussão da Posição de Calouras de Ciência da Computação* In *11º WIT - Women in Information Technology*

[15] Singh, S. (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books, 1st Edition.

[16] Blay, Eva. (2001). *8 de março: conquistas e controvérsias*. Estudos Feministas, [online]. Vol.9, n.2, pp.601-607.

[17] Stallings, W. and Brown, L. (2014). *Computer Security Principles and Practice*. Pearson, 3rd Edition.

[18] Pratini, V. (2018). *Pantera Negra: Teoria indica que Shuri pode assumir o traje do Homem de Ferro*. [Online]. Available: ⟨http://www.adorocinema.com/noticias/filmes/noticia-137993/⟩. In: April 20 2018.

[19] Santino, R. (2015). *Conheça Ada Lovelace, a 1ª programadora da história*. Available: https://olhardigital.com.br/noticia/conheca-ada-lovelace-a-1-programadora-da-historia/40718. In: April 21 2018.

[20] Numaboa, A. (2006). *A cifra de Vigenère*. [online]. Available: http://www.numaboa.com.br/index.php?option=com_content&view=article&id=506&Itemid=134. In: April 22 2018.

[21] Numaboa, A. (2005). *O código de César*. [Online]. Available: http://www.numaboa.com.br/criptografia/124-substituicao-simples/165-codigo-de-cesar. In: April 22 2018.

[22] Dantas, A. (2018). *ROT-13*. [Online]. Available: http://www.dantas.com/rot13/#oqueeh. In: April 22 2018.

[23] De Freitas, R., Nakamura F., Lauschner, T., Santos, T., Machado, A. L and Lobo, L. (2017). *Undergraduate women in Computing: where did they come from, how are they and where they are going?* In *In: LAWCC, IX Congreso de la Mujer Latinoamericana en la Computación*

[24] Nakamura F., Lobo, L., De Freitas, R., Almeida, T., Machado, A. L and Lauschner, T. (2017). *Participação feminina em cursos de computação: um estudo no Instituto de Computação da Universidade Federal do Amazonas*. In In: WIT - 11º Women in Information Technology, CSBC.