Ensinando princípios de criptografia como trote educativo e de comemoração ao dia das mulheres

Rosiane de Freitas[4], Karla Susiane Pereira[3,4], Larissa Pessoa[2,4], Ariel Bentes[2,4], Ingrid Santos[1,4], Isabelly Oliveira[1,4], 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)
Manaus-AM, Brazil

{rosiane, karla.susiane, lsp, alpb, ils, irbo, tanara}@icomp.ufam.edu.br

Abstract. *In this work we present a dynamic involving a basic method of cryptography, historically known as Caesar Cipher, which was applied to the freshmen students of the undergraduate courses in Computing of the Federal University of Amazonas. This activity happened in the first week of classes, as a way to integrate the university studentes of computing. And, taking advantage of the fact that the date of such activity coincided with the International Women's Day, March 8th, questions were also raised about the female participation in such courses. This work, therefore, aims to report the general activity performed and the applied dynamics, as well as to make considerations about the adequacy of the proposal, and how it was received and perceived by men and women university students, and the girls' participation in the constructed context.*

Resumo. *Neste trabalho é apresentada uma dinâmica envolvendo um método básico de criptografia, historicamente conhecido como Cifra de César, que foi aplicada aos alunos ingressantes de graduação em Computação da Universidade Federal do Amazonas. Tal atividade aconteceu na primeira semana de aula, como forma de integração entre os alunos calouros de Computação. E, aproveitando-se que a data de tal atividade coincidia com a Dia Internacional da Mulher, 8 de março, também foram trabalhadas questões sobre a participação das estudantes mulheres em tais cursos. Este trabalho, portanto, tem por objetivos relatar a atividade geral realizada e a dinâmica aplicada, bem como tecer considerações sobre a adequabilidade da proposta, como foi recebida e percebida, e a participação das meninas diante do contexto construído.*

1. Introdução

Todo início de ano, novos alunos universitários (popularmente conhecidos como calouros) ingressam nos cursos de graduação e se deparam com um novo ambiente de ensino, de estrutura toralmente diferente, que no geral os deixam desconfortáveis e deslocados. Dessa forma, algumas atividades de recepção aos calouros são sempre propostas pela administração da universidade e também pelos próprios alunos veteranos, com o conhecido trote, em uma atividade que culturalmente estava sendo conduzida de forma intimidadora e violenta, constrangendo ao invés de integrar e socializar, mas, que ultimamente

tem sido conduzido de forma mais autruísta, sendo mais educativo e algumas vezes de cunho social e solidário [Mitye 2018].

Com base neste novo conceito de trote educativo, foi planejada para o início do ano letivo de 2018 uma recepção aos calouros dos cursos de Computação da Universidade Federal do Amazonas (UFAM), onde a primeira semana de aula também incluía o dia 08 de março, Dia Internacional da Mulher. Assim, foi proposta uma dinâmica para o ensino de princípios de criptografia usando o médodo da Cifra de César [Paar and Pelzl 2010], tanto para integração de todos os alunos quanto para a observação da participação feminina durante o processo. Deste modo, este trabalho tem como objetivo 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. Tal dinâmica foi organizada e conduzida por professoras e estudantes do projeto Cunhantã Digital, voltado para atrair e manter mulheres nos cursos de graduação em Computação e profissões relacionadas, bem como discutir e disseminar boas práticas para esta participação [Lauschner et al. 2016] [deFreitas et al. 2016]. O uso da Cifra de César em uma dinâmica para trabalhar questões de gênero já fora conduzida em outra Instituição de Ensino Superior (IES) do Brasil [Mochetti et al. 2016] [Mochetti et al. 2017], e que serviu de base para a realização da dinâmica relatada neste trabalho, expandindo-se para turmas de mais de um curso e sendo trabalhadas questões de apresentação, formação de equipes, local de realização, encerramento da dinâmica e ações complementares, além de questões sobre participação, percepção e liderança feminina, como já destacado.

Este trabalho está organizado como segue, Na Seção 2 são apresentados os conceitos básicos de criptografia, o método da Cifra de César, variações e aplicações. Na Seção 3 a dinâmica proposta é descrita, desde o planejamento até a execução, bem como ações complementares que compuseram a atividade geral.. E, por fim, na Seção 4 são feitas as considerações finais incluindo uma análise dos resultados.

2. Cifra de César

A Cifra de César é uma técnica de criptografia usada há mais de 2000 anos, assim nomeada em homenagem ao general romano Júlio César, que utilizava a cifra a fim de proteger mensagens de significado militar. Essa codificação é uma das mais simples e conhecidas técnicas de criptografia. Trata-se de um tipo de criptografoa por substituição ou deslocamento, na qual cada letra de um texto a ser criptografado é substituída por outra letra presente no alfabeto, porém deslocada um certo número de posições à esquerda ou à direita [Paar and Pelzl 2010]. Por exemplo, se for realizado um deslocamento de quatro posições à esquerda (chave de 4), cada letra é substituída pela letra que está quatro posições adiante no alfabeto, e, nesse caso, a letra A seria substituída pela letra E, B por F, C por G, e assim sucessivamente, tal como segue:

- Mensagem original - ADA LOVELACE.
- Mensagem criptografada : EHE PSZIPEGI.

Existe uma fórmula matemática para o cálculo de qual letra substitui a letra original da palavra a codificar, sendo: $E_n(x) = (x + n)\ mod\ 26$, onde 26 é a constante que representa o tamanho do alfabeto (numerado de 0 a 25, onde $A = 0$ e $Z = 25$) , x é a letra a ser criptografada/trocada por uma outra e n é o número de trocas ou chave. Para o

exemplo acima: $E_4(A) = (0 + 4)\ mod\ 26 = 4$ (ou seja, se n for 4 e o x for A).

3. Sobre o planejmanto da dinâmica e ações complementares

A dinâmica foi aplicada para calouros dos três cursos de graduação em Computação da UFAM, sendo: (1) os cursos diurnos de Ciência da Computação (CC) e Engenharia da Computação (EC); (2) o curso noturno de Engenharia de Software (ES), cujas quantidades de homens e mulheres por curso são dadas na Tabela 1 .Assim, foi desenvolvida uma atividade pela manhã com as turmas de CC e ES, que será priorizada na descrição, e outra à noite, com a turma de ES. A seguir são dados os detalhes sobre a metodologia, planejamento, preparação e execução da atividade.

Tabela 1. Quantidades de estudantes, homens e mulheres, por curso eturno..

Curso	**Ciência Computação**		**Eng..Computação**		**Engenharia Software**	
Gênero	**Homem**	**Mulher**	**Homem**	**Mulher**	**Homem**	**Mulher**
Qtdade	52	11	52	04	41	10
TotTurno	**DIURNO: 109 (104 H e 15 M)**				**NOTURNO: 51 (41 H e 10 M)**	
TOTAL	**145 (120 Homens e 25 Mulheres)**					

O processo metodológico foi estruturado como segue. Na Parte I (atividade em sala-de-aula com cada turma em separado): (1) apresentação do Instituto de Computação (IComp), seus cursos e visão geral da UFAM; (2) apresentação dos alunos, com cada um apresentando o colega ao lado para a turma (descrever com uma ou 2 palavras o aluno do lado direito com objetivo de se verificar os critérios usados na descrição, se características físicas ou comportamentais preponderam. e então observar como descrevem as mulheres); (3) apresentação do projeto Cunhantã Digital e a importância de incentivar a participação feminina na Computação; (4) indicação da realização de uma atividade externa e entrega de uma placa com um número para cada uma das m meninas das duas turmas, em uma sequência dos m primeiros números naturais,; (5) distribuição de números para o restante (meninos), de 1 a m. Na Parte II (atividade externa em um centro de convivência): (6) formação das equipes com cada menina sendo a referência para formação e todos os alunos com números iguais compondo a respectiva equipe (com cópias do mesmo número distribuídas nas duas turmas, para gerar equipes mistas em gênero e em tipo de curso); (7) distribuir a cada grupo um copo decodificador e dar a missão de decifrarem frases, sem indicar que é a Cifra de César; (8) revelar algumas dicas, conforme o andamento da dinâmica ((a) repassar as frases codificadas e a chave; (b) dar a dica da formulação matemática; (c) dar a dica de que é a Cifra de César e explicar funcionamento). No final, ganha a equipe que decifrar o maior número de palavras no menor tempo.

Na dinâmica diurna, com 125 alunos sendo 15 mulheres, foram definidas 15 equipes sendo necessário cartelas com números de 1 a 15 feitas de cartolina e papelão; 15 decodificadores (mais 2 reservas para explicação) sendo 1 para cada equipe; 30 copos de plástico grande (500 ml); 30 tiras de papel com alfabeto completo (semelhante a uma fita métrica, mas de letras e no tamanho da circunferência de um copo). Foram necessárias 2 (duas) tiras para cada 2 (dois) copos, formando um codificador/decodificador de César; cola para colar cada fita em cada borda superior dos copos; para cada codificador/decodificador foram necessários 2 (dois) copos, cada um com uma “fita de alfabeto”

colada na borda superior; placas de cartolina reforçada com papelão para as palavras criptografadas e para as descriptografadas; 1 placa para a fórmula matemática e 1 placa para indicar ”Cifra de César”.

A aplicação da dinâmica seguiu a metodologia descrita acima, sendo realizada no Dia Internacional da Mulher (8 de março de 2018). Utilizou-se mensagens criptografadas relacionadas à Computação e ao empoderamento feminino. (1) Mulher na computação não é um bug; (2) Não é não, depois do não é tudo assédio; (3) Respeito às cunhantãs; (4) Aprender a programar e evitar que você seja programado; (5) 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, assim como o uso de celulares foram proibidos, para que fosse possível instigar a curiosidade deles e analisar quais métodos usariam para desvendar as mensagens. 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 sendo reveladas. Primeiramente, uma folha contendo a fórmula matemática da criptografia foi entregue. 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 encriptadas. Por fim, ganhou a equipe que decifrou todas as palavras no menor tempo. As 2 primeiras equipes decifraram sem dicas adicionais e a maioria das outras sem ser necessário se chegar à última dica, e com esta, todas as equipes conseguiram decifrar todas as palavras.

Como ações complementares, foram confeccionados três pôsteres smesclando mulheres famosas da história mundial e do Brasil, sendo: as pesquisadoras brasileiras Claudia Bauzer, Liane Tarouco e Clarice Souza; e estrangeiras célebres, Ada Lovelace, Grace Hooper e Katherine Johnson. Também foi confeccionado um grande quadro de *post it* com a logo da Cuhantã Digital, de modo a incentivar que todos deixassem recados alusivos ao Dia Internacional da Mulher. Ambos foram deixados durante todo o dia no hall do IComp/UFAM, atraindo interesse, comentários gerais e grande participação.

4. Conclusões e análise dos resultados

A execução da dinâmica propiciou a integração dos calouros, como desejado. Houve a integração de turmas de calouros de dois cursos diferentes de Computação, e mesmo para uma turma específica, a atividade de apresentação com a descrição do colega ao lado, propiciou momentos de descontração e maior conhecimento por todos. Foi observado tanbém as diferenças de descrições por gênero. Os alunos descreveram os colegas do gênero masculino com características comportamentais, como “legal”, ”parece gente boa”e se usava óculos, “parece ser inteligente”, “esse aí sabe programar”. Já a descrição dos meninos para as colegas do gênero feminino envolveu em vários casos atributos físicos, como “cabelo cacheado”, “estatura mediana”, ”muito bonita”.

A formação heterogênea das equipes propiciou tanto uma maior integração de alunos de cursos diferentes, como entre meninos e meninas, onde foi observou se o papel natural de liderança atribuído a menina de cada equipe (que ganhou o primeiro número de referência e a folha com a apresenação da atividade e palevras crptografadas), se manteve e como se deu sua participação. Foi observado que em algumas uma postura de lideração se manteve, com as meninas continuando a conduzirem o processo ou, pelo menos, sendo muito participativas, integradas e determinantes na resolução dos enigmas. Mas, ainda na

maioria dos casos, as meninas se mantiveram recolhidas e intimidadas, adotando somente o papel de registrar (anotar) o que ia sendo decifrado pelo restante do grupo. Mas, sem dúvida, o estímulo ao papel de líder sutilmente determinado no início ajudou na autoconfiança e participação ativa de algumas das meninas.

No final da dinâmica houve uma breve discussão com os calouros sobre o que acharam e perceberam da atividade proposta. A alegria, descontração e comprometimento de todos até o final da atividade foi uma demonstração cabal de que se envolveram e gostaram de participar, além de pontualmente afirmarem isto. Em seguida, as menimas foram chamadas à frente e parabenizadas pelo dia, e puderam se manifestar indicando que a atividade foi válida e que as fizeram analisar seus comportamentos durante a dinâmica, extrapolando para outras situações de seus cotidianos, e indicando que a partir de então iriam procurar estar atentas e trabalhar as questões discutidas. Foi dado ênfase na importância da participação mais efetiva das meninas nos cursos de computação, no que todos refletiram, se mostraram mais conscientizados e dispostos a serem mais cuidados com possíveis afirmações e comportamentos machistas, e mais engajados em dar suporte à integração das meninas. As meninas também afirmaram que iriam buscar exercer mais papéis de liderança. Por fim, pode-se constatar que uma atividade diferenciada na primeira semana de aula com propósito de integrar os alunos trouxe a sensação de pertencimento à universidade e foi bem sucedida na discussão de gênero em Computação.

Referências

deFreitas, R., Lobo, L., and Conte, T. (2016). Projeto scitechgirls: desenvolvimento de aplicativos e participação em competições de programação científicas e tecnológicas. In *Anais do XXXVI Congresso da Sociedade Brasileira de Computação (CSBC 2016). X Women in Information Technology (WIT)*, pages 2723–2727, Disponível em: http://ebooks.pucrs.br/edipucrs/anais/csbc/assets/2016/wit/20.pdf. SBC.

Lauschner, T., deFreitas, R., Nakamura, F., and Lobo, L. (2016). Cunhantã digital: programa de incentivo à participação de mulheres da região amazônica na computação e áreas afins. In *Anais do XXXVI Congresso da Sociedade Brasileira de Computação (CSBC 2016). X Women in Information Technology (WIT)*, pages 2656–2660, Disponível em: http://ebooks.pucrs.br/edipucrs/anais/csbc/assets/2016/wit/05.pdf. SBC.

Mitye, C. (2018). A nova cara do trote universitário. Disponível em: http://mundoeducacao.bol.uol.com.br/educacao/.

Mochetti, 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 *Anais do XXXVII Congresso da Sociedade Brasileira de Computação (CSBC 2016). XI Women in Information Technology (WIT)*, pages 1186–1189. SBC.

Mochetti, K., Salgado, L., Zerbinato, A., Souza, B., and Avelino, M. (2016). Ciência da computação também é coisa de menina! In *Anais do XXXVI Congresso da Sociedade Brasileira de Computação (CSBC 2016). X Women in Information Technology (WIT)*, pages 2647–2651, Disponível em: http://ebooks.pucrs.br/edipucrs/anais/csbc/assets/2016/wit/03.pdf. SBC.

Paar, C. and Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer-Verlag, Berlin Heidelberg, 1st ed. edition.