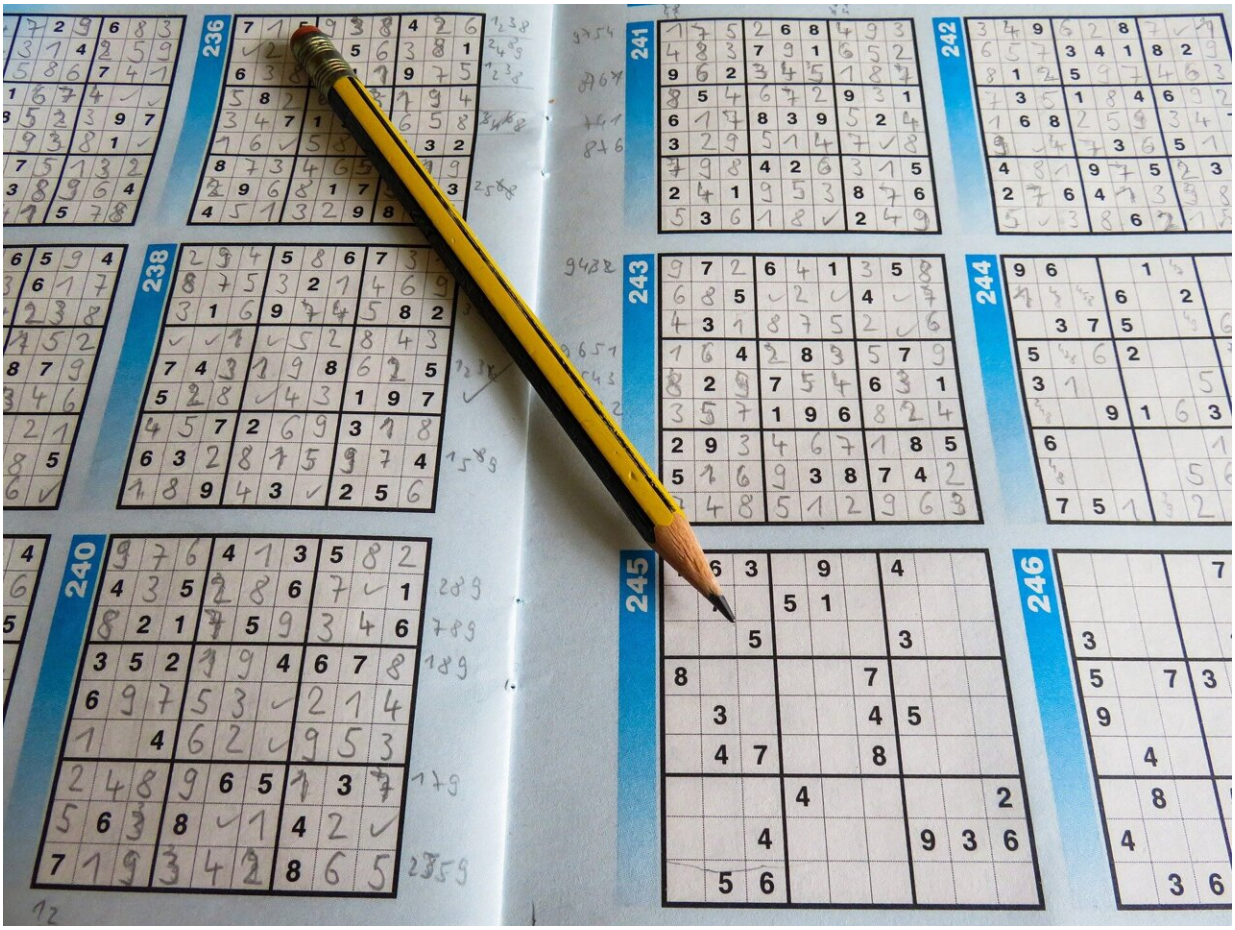
A new message encryption scheme inspired by the Sudoku puzzle

August 11 2023, by David Bradley



Credit: Pixabay/CC0 Public Domain

A novel advance in data security is discussed in the *International Journal*

of Information and Computer Security in which the Japanese puzzle known as Sudoku promises a cryptographic system for text information that works even in situations where computational power is limited. The approach could have applications in devices with constrained computer resources such as radio-frequency identification devices (RFID), medical and health care instruments, remote sensing networks, and smart cards.

Shadi R. Masadeh of the Department of Cyber Security at Isra University, in Amman, Jordan, Hamza Abbass Al-Sewadi of the Computer Technology Engineering Department at Iraq University College, in Basrah, and Mohammad Abbas Fadhil Al-Husainy of the Al-Maaqal University also in Basrah, Iraq, demonstrate how the dynamic nature of the Sudoku puzzle can be used as the basis of a secret encryption key, or cipher, to unlock a new approach to securing sensitive information.

The dynamic nature of the approach significantly boosts the security of the system. The team's experimental results demonstrate that this approach is superior to other experimental lightweight cryptography.

The strength of MESP lies in its extensive key space and its superiority in frequency analysis probability when compared to alternative techniques. While sharing a similar character count with Verma's algorithm, MESP boasts a substantially wider key space. Furthermore, the algorithm's flexibility is evident in its ability to accommodate a broader range of characters.

This adaptability is achieved by expanding the size of the index tables, making room for all conceivable characters within a language, and even accommodating multiple languages. The system adheres to Shannon's principles of confusion and diffusion so that the substitution and transposition steps seamlessly blend, providing a strong defense against

security breaches.

In today's landscape of symmetric cryptosystems, the fusion of ideas from the Sudoku puzzle, pseudo-random number generation, and dynamic permutation introduces a versatile and potent security technique. The implications stretch across various domains, from fortified health care data security to more resilient smart cards and remote sensing networks. Backed by compelling experimental results, this algorithm, which the team calls "Message Encryption (inspired by) Sudoku Puzzle," heralds a new era in lightweight cryptography, beyond its "puzzling" origins.

More information: Shadi R. Masadeh et al, A message encryption scheme inspired by Sudoku puzzle, *International Journal of Information and Computer Security* (2023). DOI: 10.1504/IJICS.2023.132739

Provided by Inderscience