The 8th Workshop in Primary and Secondary Computing Education. Aarhus (Denmark), November 11-13, 2013

Scout patrol secret grilles

One more CS Unplugged-style activity on cryptography

Jenny's scout patrol is in deep trouble.
The girls used to encrypt their messages simply by writing them backwards.
But it is not a secret any more.

Jenny, the best mathematician in the team, was asked to suggest a better cipher.

Inspired by "Computer Science Unplugged" project that is aimed at presenting important topics in computing, without using computers, we have developed a new supplementary activity on symmetric key encryption.

One may use the activity to give a broader understanding of the Internet web browser secure communication concepts (e.g. session key strength, session key exchange) to K-12 students.

Activity description

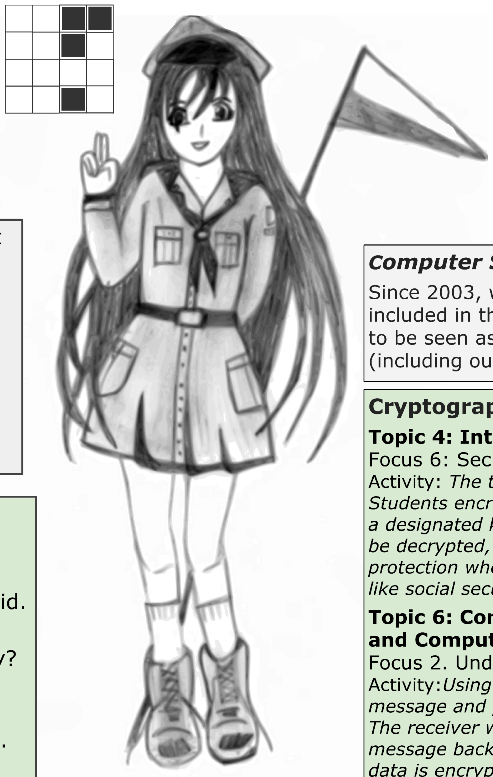
1. Students are asked to decrypt Jenny's message. They are told that she's used a rotating 4 x 4 grille and they remove four square holes from a 4 x 4 grid.

They try to discover the rules one can use for decoding. It may turn out not to be so simple. Why? Finally the unencrypted words should appear.

2. The next challenge for students is to make up their own grilles and to encrypt their own message.

The first attempt usually fails…
It's not easy to discover distribution rules of holes.

3. The extension exercises included in the activity text, dedicated for older studentes, are:
– to consider the number of "worse" 4 x 4 grilles (seen as figures with a reflection symmetry);
– to consider the total number of 4 x 4 grille-keys (students may imagine Jenny's enemy who knows the grille method and uses an exhaustive search);
– to analyse the problem of the distribution of Jenny's grilles as an example of the problem of key exchange (Jenny's patrol uses ...map of bits);
– to devise an attack exploiting the weaknesses of the grilles (related to a rotational symmetry).



C	R	O	U
N	Y	E	N
T	E	R	D
W	P	D	S

"A central theme in cryptography is what we do *not* know or can*not* do. The security of a cryptosystem often rests on our inability to efficiently solve a problem in algebra, number theory, or combinatorics.

Thus, cryptography provides a way to counterbalance the impression that students often have that with the right formula and a good computer any math problem can be quickly solved."

Professor Neal Koblitz

Computer Science Unplugged-style

Since 2003, when CS Unplugged-style approach was included in the ACM K-12 Model Curriculum, it has started to be seen as the basis of new philosophy for teaching (including outreach) CS without using a computer.

Cryptography in ACM K-12 Model Curriculum

Topic 4: Internet Concepts
Focus 6: Security on the Internet
Activity: *The teacher creates several different encryption keys. Students encrypt messages to one another using a designated key. The message is sent to another student to be decrypted, but the key is not. Discussion follows regarding protection when providing personal identification information like social security numbers and credit card numbers.*

Topic 6: Connections Between Mathematics and Computer Science
Focus 2. Understanding various forms of encryption
Activity:*Using a simple form of encryption, encrypt a text message and pass it to a classmate, along with a key. The receiver will use the key to translate the encrypted message back to the original text. Discuss the reasons why data is encrypted.*

Level 2 Objectives and Outlines. CSTA 2006

Turning grilles in fiction and history

A 6 x 6 grille is used by Mathias Sandorff, the character of the novel by Jules Verne (1885).

Verne gives a very good description of the system. He tells his readers that such a cipher is ...unbreakable unless you have the grille.

Verne had come across the idea in Baron Fleißner's (a retired Austrian cavalry colonel) *Handbuch* (1881).

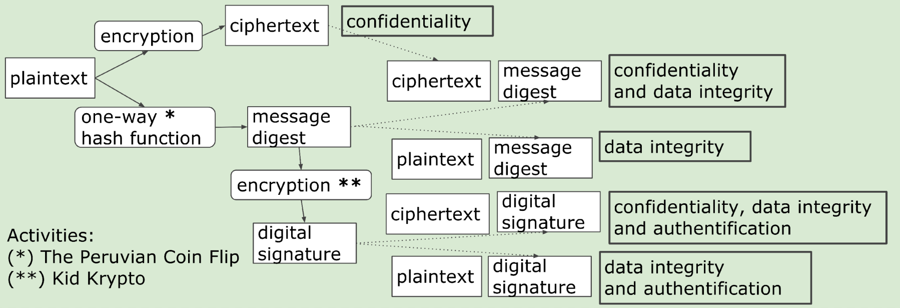
The grilles (in various sizes) were used by the German army at the end of 1916 (till French cryptanalysts devised attacks exploiting the weaknesses of the grilles).

Activity evaluation

The activitiy conforms to most of Unplugged pattern characteristics: (1) it uses no computers but only inexpensive equipment, (2) it tells a story to engage pupils, (3) it involves interaction with other classmates (cooperation and competition), (4) it encourages students to discover answers by trial and error, (5) is primarily focused on outreach rather than teaching.

The activity was tested with teenagers during several computing school lessons and a university science festival. The feedback from the students was universally positive. After some adjustments to make the activity more engaging, it was published in a professional journal for Polish mathematics teachers.

Internet cryptography. CS Unplugged activities on cryptography



Activities:
(*) The Peruvian Coin Flip
(**) Kid Krypto

Authors
Paweł Perekietka, pawel.perekietka@gmail.com
Klaudyna Potocka Lyceum, Teachers Training Centre, Poznań, Poland
Agnieszka Kukla, agnieszka.kukla91@gmail.com
Przemysław Pela, pelas@wmi.amu.edu.pl
Faculty of Mathematics and Computer Science,
Adam Mickiewicz University, Poznań, Poland

http://goo.gl/FVGlPb

References (selected)

[1] V. Ahuja, Network and Internet security, Academic Press Professional, Inc., 1996.
[2] N. Koblitz. Cryptography as a teaching tool, Cryptologia, Vol. 21, No 4, 1997.
[3] T. Nishida, S. Kanemune, Y. Idosaka, M. Namiki, T. Bell, and Y. Kuno. A CS unplugged design pattern, *Proceedings of the 40th ACM Technical Symposium on Computer Science Education*, SIGCSE 2009, pp. 231-235, 2009.
[4] W. Wajnert. Przygody z Machefim, SIGMA-NOT, 1983.

We are grateful to Łukasz Nitschke for his insightful comments and to Agnieszka Dorywała for her drawing. We also thank Elżbieta Przybył, and many others for their support.

Dedicated to the Polish men and women who first broke the Enigma codes in the 1930s