© TAKASU/FOTOLIA

Cryptography
Legal Hacking

BY BRETT KRAABEL

Authorities constantly have to lengthen credit card security keys to prevent fraud.

CNRS researchers recently solved a 40-year-old puzzle by decoding one variant of the discrete logarithm problem, a formula that is used to secure objects like RFID tags.[1] Why would researchers spend public money trying to hack security algorithms? To show that cryptographic methods based on these algorithms are vulnerable to modern computing attacks, and warn authorities not to use them in security applications.

All security algorithms are based on formulas that take a clear (i.e., uncoded) symbol as input and, by using a number called a "key," return a coded symbol as output. For a given input, different keys will produce different outputs and, without knowing which key is used, it is virtually impossible to determine the original message from the encoded one.

A good algorithm is one whose security can be improved simply by increasing the number of bits in the secret key. For instance, the key used for credit-card security algorithms is regularly lengthened to combat the ever-increasing computing power of hackers. In 2009, this key length was doubled, meaning that instead of one year, it would now take a million years to crack the code. If this change in key length only resulted in doubling the time it would take to crack the code, then the security algorithm could not stay ahead of computing power. Thus, when attacking a cryptographic method, explains Pierrick Gaudry from the Loria,[2] "the Holy Grail is to find an attack algorithm whose computation time increases [almost in proportion to] the number of bits in the key." For a variant of the discrete logarithm problem, Gaudry and colleagues did just that: they devised an attack algorithm whose calculation time increases almost in proportion to the number of bits in the key.

This has led authorities to withdraw their endorsement for using this discrete logarithm variant in cryptography and has provided a new algorithm with which to test other cryptographic methods. "We protect citizens by guaranteeing the security of cryptographic applications," concludes Gaudry. II

1. R. Barbulescu et al., "A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic," *Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science*, 2014. 8441: 1-16. 2. Laboratoire lorrain de recherche en informatique et ses applications (CNRS / Université de Lorraine / Inria).

✉ pierrick.gaudry@loria.fr

Biology
Fighting Malaria Relapse

BY EMMA WALTON

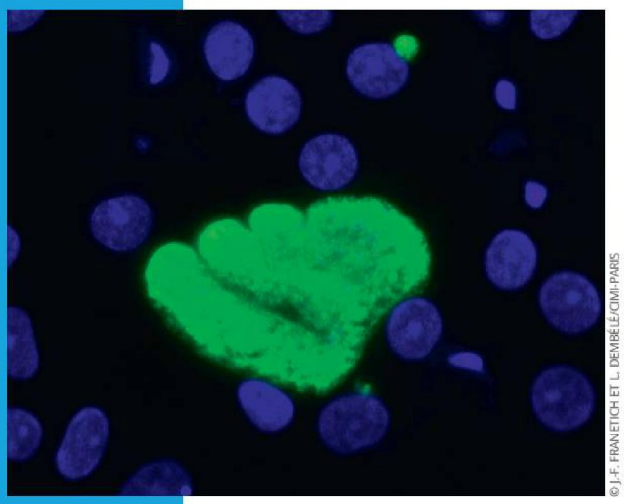
Many people who have had malaria can relapse years after the initial infection. Such relapses are due to a dormant form of the parasite, so far poorly accessible to researchers. Now, a team led by Georges Snounou[1] and Dominique Mazier[2] has succeeded in cultivating it for the first time.[3]

Malaria is caused by *Plasmodium*, a single-cell parasite carried by the mosquito *Anopheles*. Following a bite from an infected mosquito, tiny parasitic sporozoites enter the bloodstream and pass into the liver. There, they multiply to form thousands of merozoites that enter the red blood cells and cause the symptoms of malaria. Two species of *Plasmodium*, *P. vivax* and *P. ovale*, also produce dormant forms in the liver. Named "hypnozoites," they can wake up without warning and induce relapses.

So far, the study of hypnozoites has involved infected monkeys and "the occasional, gallant volunteer," says Snounou. But as he points out, the ratio of hypnozoites to liver cells is so low that studying them is like looking for a needle in a haystack. An ideal model would consist of infecting liver cells in a dish. Yet "liver cells fail to grow in culture," explains Mazier, and infection with *Plasmodium* causes many cells to detach and die. Now, by adding liver cancer cells to plug the holes left by dying cells and providing a soft support, Mazier's team has managed to grow infected cells in culture for up to 40 days, approximately four times longer than previous attempts.

The model was put to the test by screening for anti-hypnozoite compounds. Interestingly, one molecule awakened some of the hypnozoites. This led to a therapeutic strategy called "wake and kill," involving one drug to awaken the hypnozoites, and another to kill them. "This may be the key to a radical cure," concludes Mazier.

1. Centre d'immunologie et des maladies infectieuses (INSERM / Université Pierre et Marie Curie / CNRS). 2. Service de parasitologie-mycologie (AP-HP / Hôpitaux Universitaires Pitié-Salpêtrière). 3. L. Dembélé et al., "Persistence and activation of malaria hypnozoites in long-term primary hepatocyte cultures," *Nat. Medicine*, 2014. doi: 10.1038/nm.3461.



© J.-F. FRANETICH ET L. DEMBÉLÉ/CIMI-PARIS

In liver cells, the parasite *P. cynomolgi* can form thousands of merozoites ready to infect blood cells (large green shape), or stay in a dormant form (small green dot).

✉ dominique.mazier@psl.aphp.fr
georges.snounou@upmc.fr