Patrick Ray Sapusao
In Anderson's paper, "Why Cryptosystems Fail,"

1. How does he claim that the threat model commonly used by cryptosystem designers was wrong?
Most threat model used by the designer was wrong because designers concentrated on what could possibly happen rather than on what was likely to happen, most frauds were not caused BY technical attacks, but by implementation errors and management failures.

2. What is the status of the banking security system in terms of encryption?
Most ATMs operate using some variant of a system developed by IBM. This uses a secret key, called the 'PIN key', to derive the PIN from the account number, by means of a published algorithm known as the Data Encryption Standard(DES). The result of this operation is called the 'natural PIN', an offset can be added to it in order to give the PIN that the customer must enter. Thus making the security of the system depends on keeping the pin a secret. The most standard method to this problem is a security module, A PC in a safe, and it is programmed to manage all the bank's keys and PINs in such a way that the mainframe programmers only ever see a key or PIN in encrypted form. Banks that belong to the VISA and Mastercard ATM networks are supposed to use security modules, in order to prevent programmers to know the pin of the customer

3. Anderson constituted what problems in the current encryption products as of his writing?
The first problem is thus that the hardware version of the security modules does not get bought at all, either because it is felt to be too expensive, or because it seems to be too difficult and time-consuming to install, making banks end up using a software as a security module which can open new problems, the most obvious, the problem with software PIN encryption is that the PIN key can be found without too much effort by system programmers.

Not all security products are equally good, and very few banks have the expertise to tell the good ones from the mediocre ones. Some security modules can be easier to attack compared to others, most security modules designed to avoid employees to reach the cryptographic keys but the enclosure of the security module can be penetrated physically.

Even when you purchased better products, there are many ways in which poor implementation or sloppy operating procedures can leave the bank exposed.

4. What was/were the implication/s of Anderson's findings in his paper?
Equipment vendors argue that real security expertise can only be found in universities, government departments, or specialist consulting firms and because of this shortage, only huge projects have the capability to hire security shortage during the development or implementation process. This may result in companies and government departments buying whatever products have been recommended by the authority and because they lack skills to implement or manage security features it can lead to systems with holes

5. In synthesis and in your own comprehension of the article, why cryptosystems fail? And with all these, what is next in cryptology?
This lack of feedback has led to a false threat model being accepted. Designers focussed on what could possibly go wrong, rather than on what was likely to happen, and many of their products are so complex and tricky to use that they are rarely used properly.

A paradigm shift is underway where a fusion of security and software engineering and for me, I think in the future should we aim to automate the security process, we should focus on improving our cryptology where we can achieve real anonymity and no one can really see the pin code including the hashed one to minimize breaches and we should also strategies to cope with diversity.