The details of Electronic Cash

How does Alice's bank "sign" her enciphered money order?

Let's say the bank uses RSA with keys n, e, d.

Let the money order be M

Alice chooses a random k in $1 < k < n$.

Alice "blinds" (enciphers) the money order by computing $t = Mk^e \bmod n$.

Bank signs t as

$$t^d \equiv (Mk^e)^d \equiv M^D k^{ed} \equiv M^d k \pmod{n}.$$

Alice "unblinds" (deciphers) the signed money order t^d by computing $k^{-1} \bmod n$ (via extended Euclid) and multiplying:

$$s = t^d k^{-1} \bmod n \equiv (Mk^e)^d k^{-1} \equiv$$

$$\equiv M^d k^{ed-1} \equiv M^d \pmod{n}.$$

To "open" (decipher) the 99 t, Alice tells the bank M and k for each. The bank verifies that each $t = Mk^e \bmod n$.

Secret splitting (used in key escrow):

Let the secret be s.

Choose a random r of the same length as s.

One party gets r; the other gets $r \oplus s$.

Together the two parties can compute $r \oplus (r \oplus s) = s$.

“Bit commitment”

Alice wants to commit to a “bit” (it can be a string) now so that she can’t change it later, but only Alice knows it for now.

Alice commits to b by generating two random strings R_1, R_2.

She creates a message (R_1, R_2, b) and computes a hash (SHA. say) of it.

She reveals (or tells Bob) the hash value and R_1.

When the time comes to reveal b, Alice shows the message (R_1, R_2, b).

Bob checks that R_1 is the same as it was earlier and verifies the hash value.

Why is R_2 needed? Because if b were a short string (one bit, literally, say), then Bob could guess it from the hash value.

Remarks on Protocol 4:

It is not transferable or divisible.

Can Alice cheat? She can copy her $1000 money order. The first time she spends it is okay. But she gets caught the second time she spends it.

Can she create a money order with a bad id string? One chance in 100.

Alice can't change the 20-digit number or the identity strings, because then the bank's signature would no longer be valid.

Can the merchant cheat? No.

Can the merchant and Alice collude to spend the e-cash twice? No, because they can't change the 20-digit number signed by the bank, so the bank will not have to pay the $1000 more than once.

Can Eve copy Alice's money order and spend it first? Yes. It is like cash.

Even worse, if Alice didn't know that Eve copied it and spent it, then Alice would be caught when she spent it the first time.

Eve could eavesdrop on communication between Alice and the merchant and deposit the money (as a merchant) before the merchant deposits it. When the merchant tries to deposit it, he will be found as a cheater.

Both Alice and the merchant must protect their e-cash as if it were cash. It must be enciphered when it is send across the Net.

The Perfect Crime

1. Alice kidnaps a baby.

2. Alice prepares 10,000 anonymous money orders for $1000 each.

3. Alice blinds them, sends them to authorities, and demands that

a. a bank signs all 10,000 money orders, and

b. the results be published in a newspaper.

4. The authorities comply.

5. Alice buys the newspaper, unblinds all the money orders and spends them.

6. Alice frees the baby.

Note that there is no physical contact.