1 On Replacing Humans by Cryptography

Prologue: a telephone operator has fired 90% of its personnel and replaced call centers with web services. Now, customers have to go on the web over the Internet to manage their contract with the operator. This requires secure communications. The operator also removed paper-based mailings. Customers now receive invoices directly from their bank and announcements by email.

1. When a customer visits the operator's web site, how can he/she authenticate the operator?
2. Once a secure connection with the operator is established, the operator must authenticate the customer. Unfortunately, the restructuring was made in a rush and the operator did not provide any password nor any authenticating facilities to the customers.
   (a) Identify another usable communication channel between the customer and the telephone operator which can still provide some kind of security. In what follows we assume that this channel provides no confidentiality but authentication from the customer to the operator.
   (b) We now have two communication channels at disposal: the link A which provides secure communication in which the customer has authenticated the operator and the identified channel $B(\mathsf{ID})$ from the previous question which provides authentication from the customer of identity ID to the operator. We consider the following protocol.

Customer ID		Operator
	$\xrightarrow{A:\mathsf{ID}}$	receive ID', generate a password w
receive w'	$\xleftarrow{A:w}$	insert $(\mathsf{ID}', w, \mathsf{time})$ in a list L
	$\xrightarrow{B(\mathsf{ID}):\mathsf{ok}}$	receive ok from a channel $B(\mathsf{ID}'')$
		if there is a tuple (ID'', w'', t) in L with $t > \mathsf{time} - \Delta$,
password: w'		extract it and validate account (ID'', w'')

   In this protocol, time denotes the clock value and Δ denotes a maximum time delay after which a password request session expires on the server side if not completed. After the protocol completes, the customer can authenticate through the A link by using a password.
   Show how an adversary can mount an attack in which he/she can log in an account of identity ID.
   (c) We fix the previous protocol by using a session identifier s as follows.

Customer ID		Operator
		increment a counter s
	$\xrightarrow{A:\mathsf{ID}}$	receive ID', generate a password w
receive $s'\|\|w'$	$\xleftarrow{A:s\|\|w}$	insert $(s, \mathsf{ID}', w, \mathsf{time})$ in a list L
	$\xrightarrow{B(\mathsf{ID}):s'}$	receive s'' from a channel $B(\mathsf{ID}'')$
		if there is a tuple $(s'', \mathsf{ID}'', w'', t)$ in L with $t > \mathsf{time} - \Delta$,
password: w'		extract it and validate account (ID'', w'')

   Show that if the account is validated and the customer of identity ID'' is honest, only this customer can have received the password w''.
3. The operator, which definitely has some liquidity problems, stops paying for certificates. How can we now launch secure communications over the Internet from a customer to the operator?
4. A malicious worm circulates and collect passwords of customers. Which action must be taken by the operator?

Epilogue: finally, the operator, which survived thanks to some financial support by the government, fired his cryptographers and launched a new call center in Asia.

2 ID Cards with Cryptographic Keys

The government would like to set up a public key infrastructure for every citizen. For this, some identity cards are given. We assume that ID cards have a tamper proof chip with a protected secret key inside and a scannable public key.

1. Assuming that the public key can be freely scanned by radio link, what is the threat for citizens?
2. We now assume that public keys are based on identity, i.e. there is a master public key which is common for every one and the citizen's public key is simply its name as it appears on the ID card. Secret keys are used to sign legal documents.
   Recall how secret keys are made. What is the major threat for citizens?
3. We now assume that the secret key is generated by the chip itself once it is switched on for the first time and that the public key is printed on the ID card and scannable by visual contact only. Again, the secret key is used to sign legal documents. More concretely, there is a button "sign" on the ID card. The chip receives the document to be signed by radio link, and if the button is pressed, the chip signs the document and sends the signature by radio link as well.
   (a) We assume that payments in shops are made by payment orders signed by the ID card. How can a shop overcharge a customer?
   (b) We assume that payment orders are short messages and that there is now a display on the ID card which displays messages to be signed. Assume that vendors now always ask for the ID card for payments.
   What is the threat for citizens?
4. We now assume that digital signatures are no longer used, but that identity-based encryption is implemented. Concretely, a message for a citizen can be encrypted by using the master public key and his/her identity as it displays on the card. The encrypted message can be sent to the chip on the ID card by radio link so that it can be decrypted by using the sealed secret key. The decrypted message is simply displayed on the card, but the card always remains silent on radio channels.
   Propose a scheme so that any organization can authenticate any citizen over the telephone.