PART 1: CRACKING THE ULTRA-SECURE DIEBOLD CENTRAL VOTE DATABASE PASSWORD

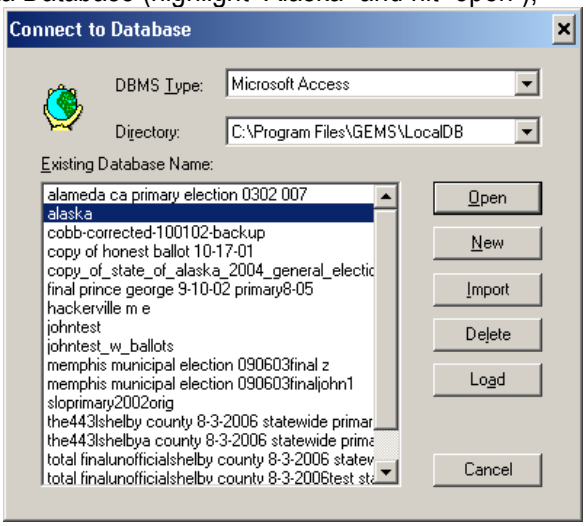
By John Brakey AUDITAZ@cox.net and Jim March 1.jim.march@gmail.com May 15, 2007

Excerpt from a letter written to Pima County Manager Charles Huckelberry January 10, 2007 from William J. Risner Attorney at Law

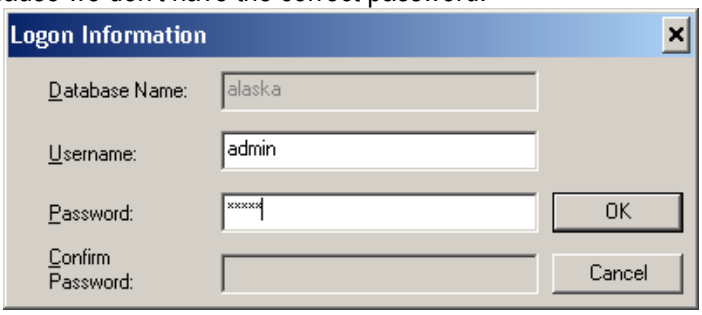
…"Every study of the security of computer voting systems has identified insiders such as company employees and election department employees as the primary security risks. Local political parties are never named. It is those with access that are of primary concern. Our party has been a leader in promoting security."…

How to enter a GEMS database without the correct password:

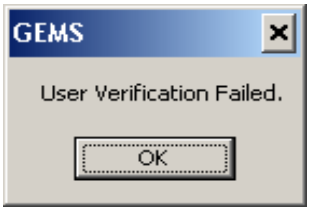
1) Let's try to open the Alaska Database (highlight "Alaska" and hit "open");



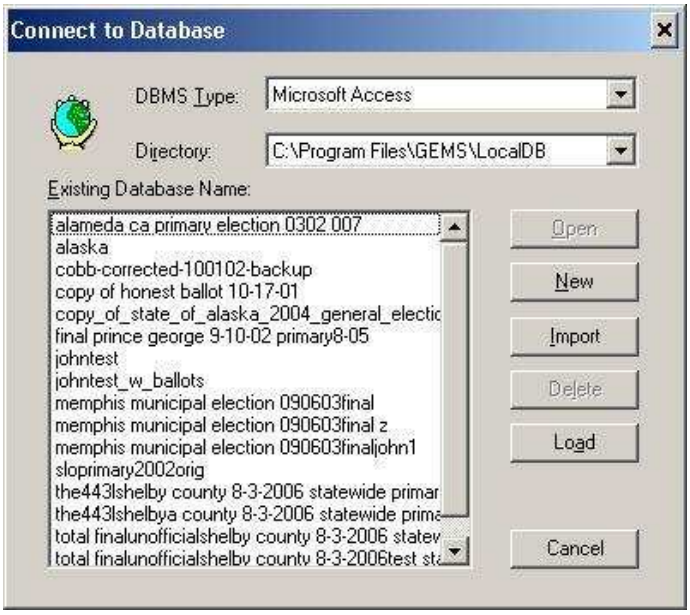
2) It won't open because we don't have the correct password:



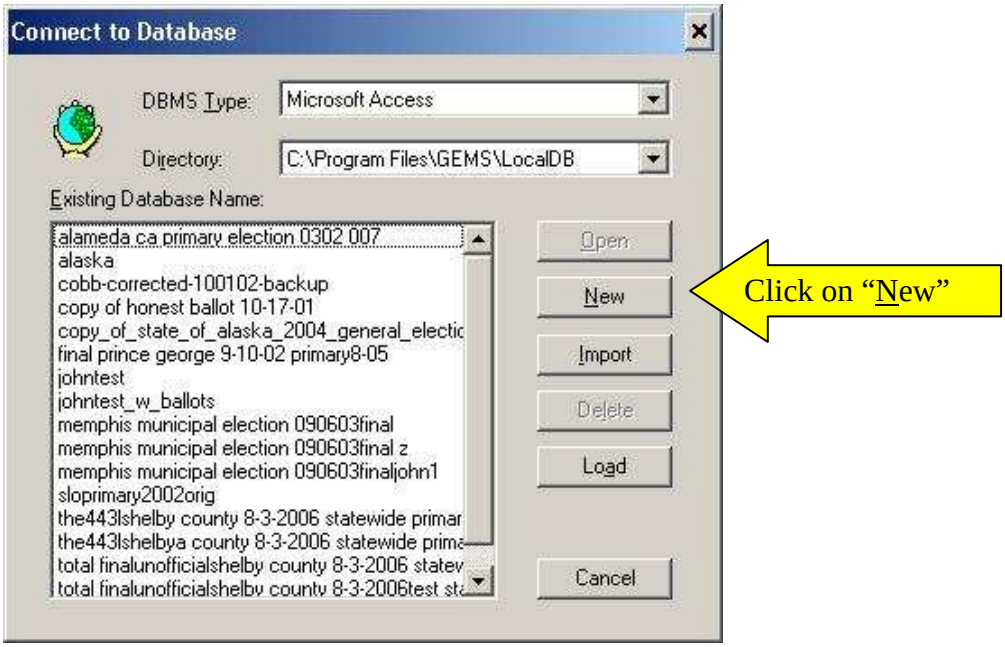
3) So we get an error...



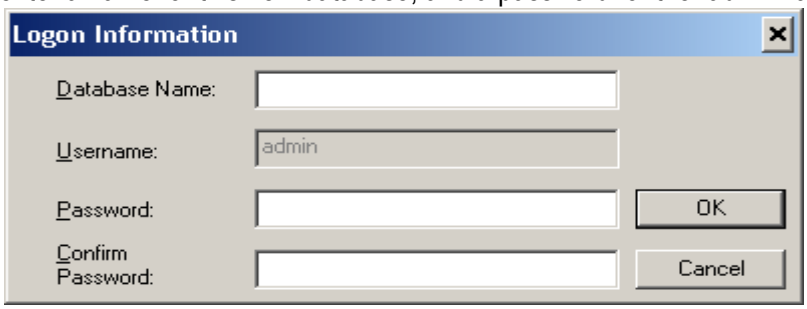
4) Open GEMS:



5) Then click on “New” to create a new election data file...



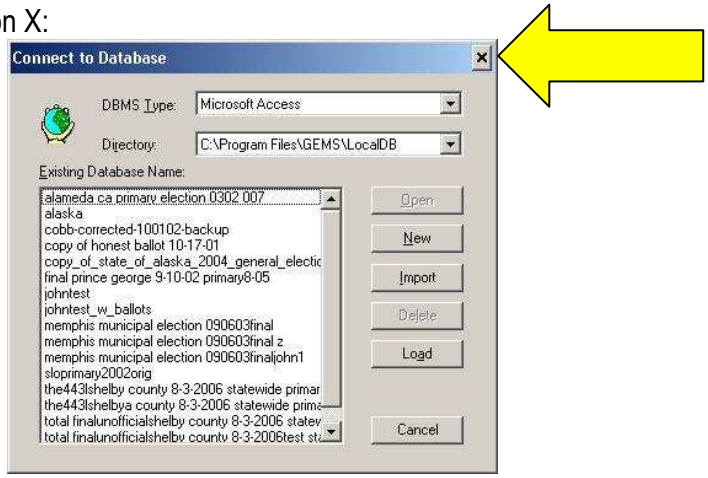
6) We have to enter a name for this new database, and a password for the “admin” account:



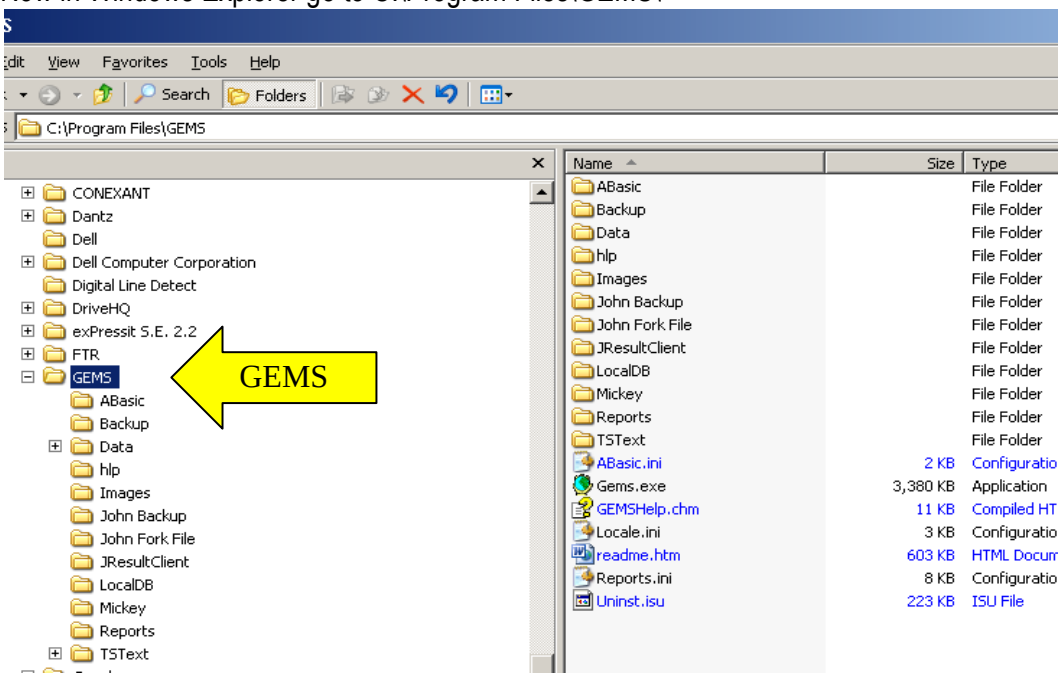
7) Enter the new data file name and password then click “OK” - we're going to enter a password (twice) of “test”:

8) Just close the next screen when it opens up the GEMS program (not shown, use the “go away-X” same as in the next point below...)

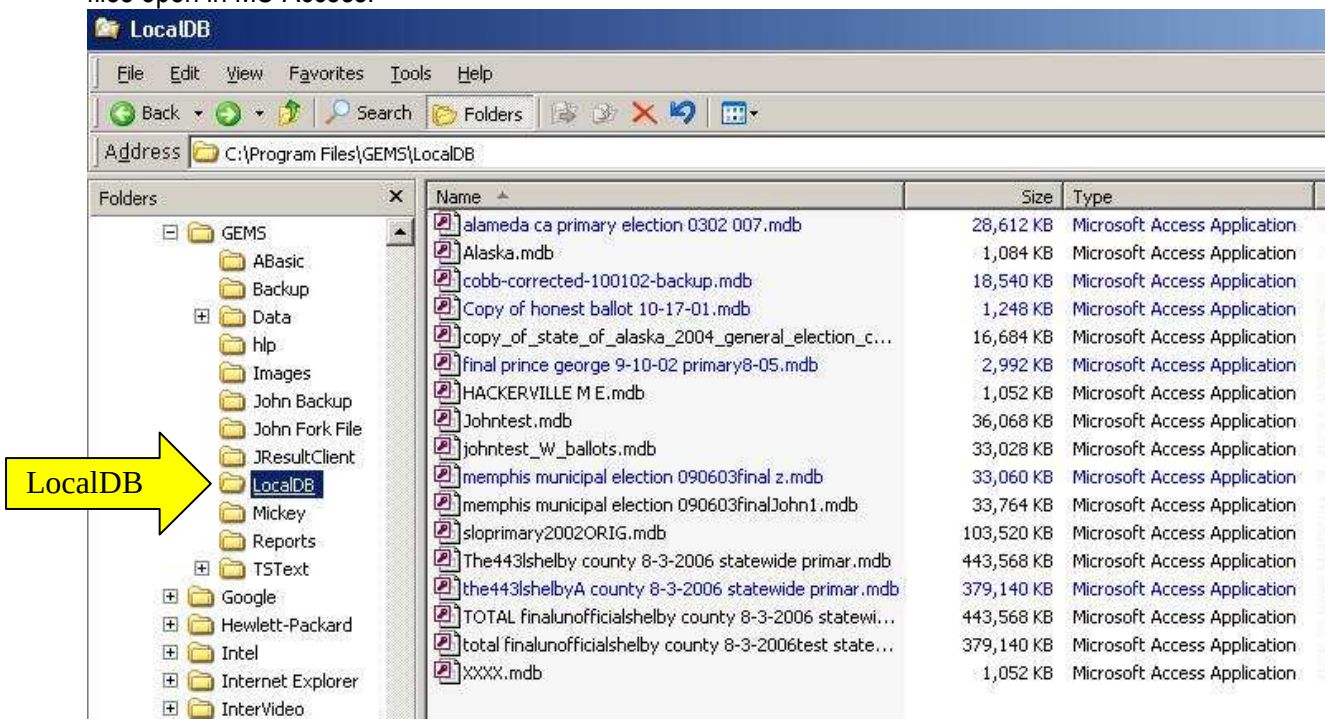
9) Close Gems by clicking on X:



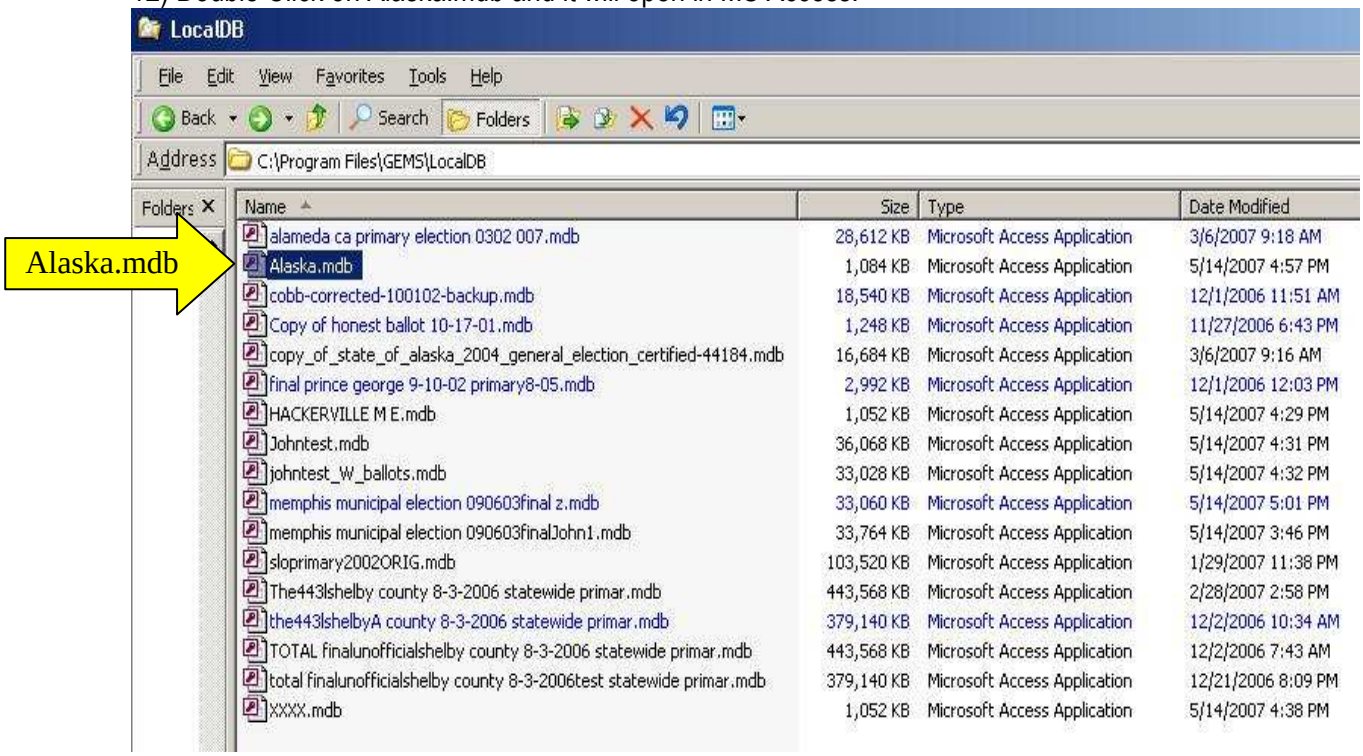
10) Now in Windows Explorer go to C:\Program Files\GEMS\



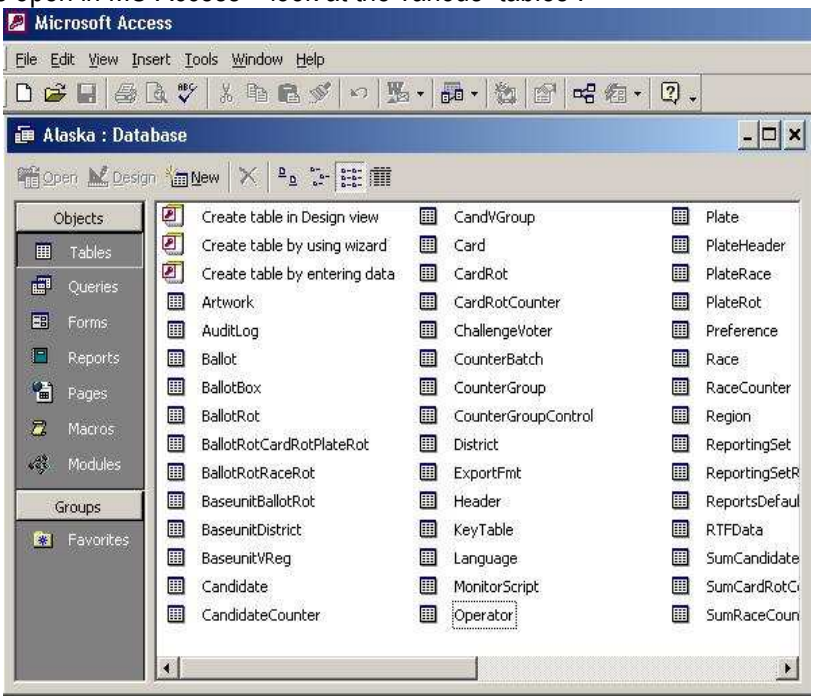
11) Go down column and click on Local DB (C:\Program Files\GEMS\LocalDB) - all of these data files open in MS-Access:



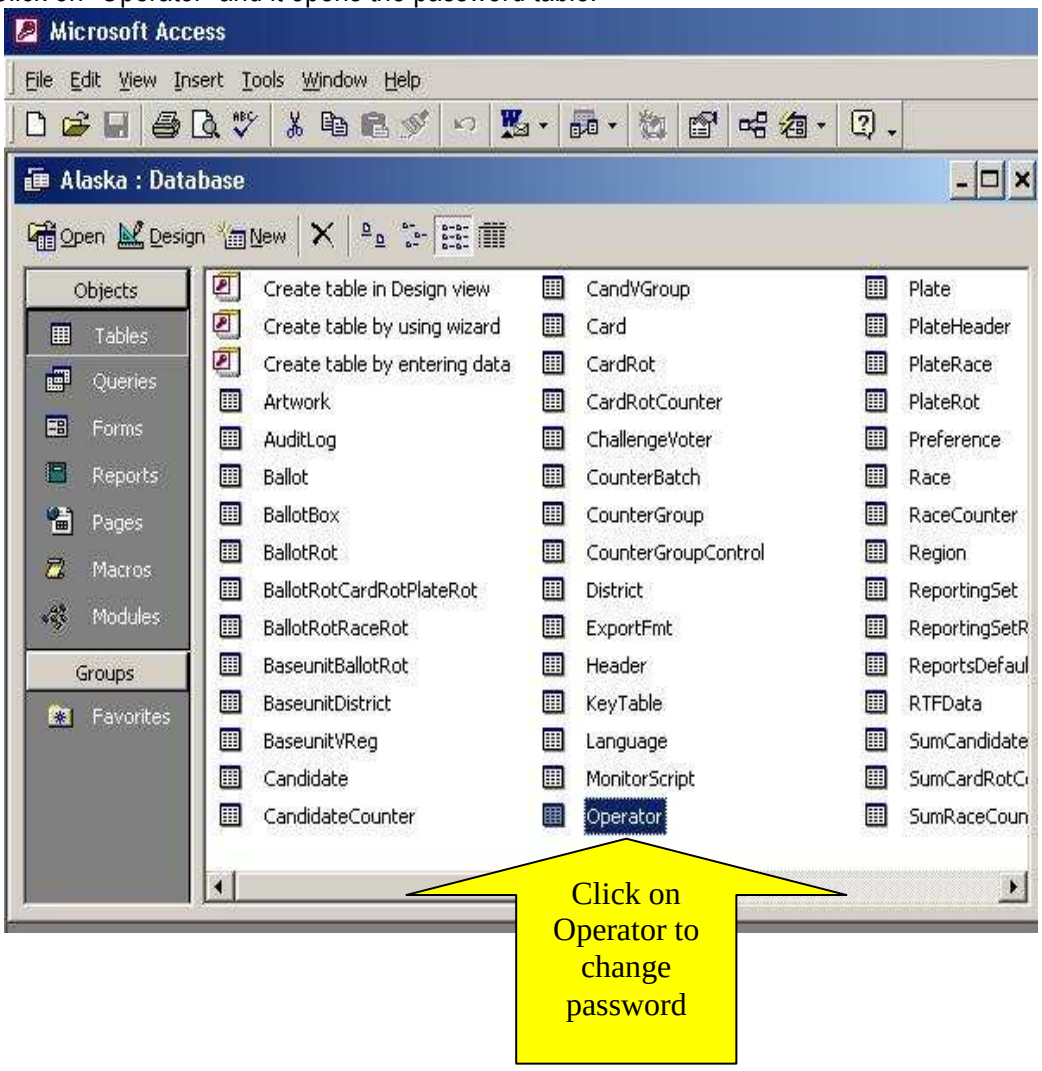
12) Double Click on Alaska.mdb and it will open in MS Access:



13) GEMS files open in MS-Access – look at the various “tables”:



14) Click on “Operator” and it opens the password table:



15) As you can see the entire password is encrypted (“scrambled”):

t Access - [Operator : Table]

View Insert Format Records Tools Window Help

d	Label	FullName	Password	AccessLevel	RegionId
0	admin	admin	Rptasa4PefgXk	0	0
1	User 1	Region I User	xw8u2xwG.gpmg	1	1
2	User 2	Region II User	8Z5xfKoTrnBw6	1	2
3	User 3a	Region IIIa User	2MWG7trrDTWk6	1	3
4	User 3b	Region IIIb User	jgrC3MgpJVz/Y	1	4
5	User 4a	Region IVa Use	NzFvDHpLJJcu.	1	5
6	User 4b	Region IVb Use	xOOQXxKXAYNT6	1	6

16) Now go back to Windows Explorer and open the database we created called Hackerville M E (C:\Program Files\GEMS\LocalDB) and do the same process to view the “scrambled version” of the password we created (test):

alDB

Edit View Favorites Tools Help

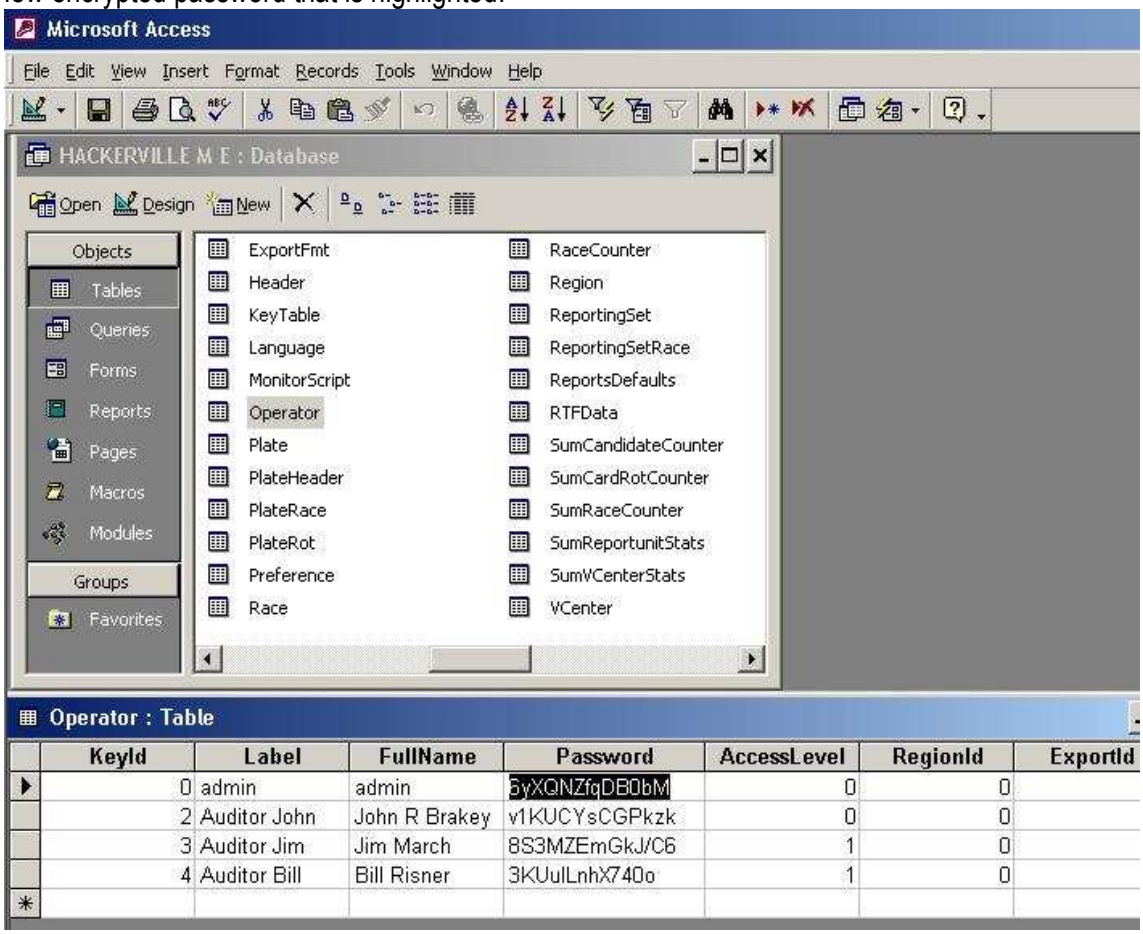
Search Folders

C:\Program Files\GEMS\LocalDB

Name	Size	Type
alameda ca primary election 0302 007.mdb	28,612 KB	Microsoft Access Application
Alaska.mdb	1,084 KB	Microsoft Access Application
cobb-corrected-100102-backup.mdb	18,540 KB	Microsoft Access Application
Copy of honest ballot 10-17-01.mdb	1,248 KB	Microsoft Access Application
copy_of_state_of_alaska_2004_general_election_certified-44184.mdb	16,684 KB	Microsoft Access Application
final prince george 9-10-02 prim 8-05.mdb	2,992 KB	Microsoft Access Application
HACKERVILLE M E.mdb	1,080 KB	Microsoft Access Application
Johntest.mdb	36,068 KB	Microsoft Access Application
johntest_W_ballots.mdb	33,028 KB	Microsoft Access Application
memphis municipal election 090603final z.mdb	33,060 KB	Microsoft Access Application
memphis municipal election 090603finalJohn1.mdb	33,764 KB	Microsoft Access Application
sloprimary2002ORIG.mdb	103,520 KB	Microsoft Access Application
The443lshelby county 8-3-2006 statewide primar.mdb	443,568 KB	Microsoft Access Application
the443lshelbyA county 8-3-2006 statewide primar.mdb	379,140 KB	Microsoft Access Application
TOTAL finalunofficialshelby county 8-3-2006 statewide primar.mdb	443,568 KB	Microsoft Access Application
total finalunofficialshelby county 8-3-2006test statewide primar.mdb	379,140 KB	Microsoft Access Application
XXXX.mdb	1,052 KB	Microsoft Access Application

Hackerville M E

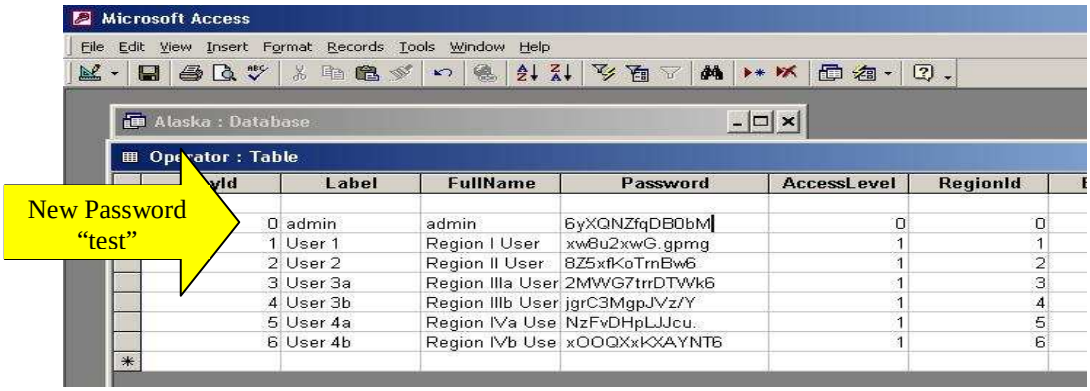
17) This shot shows the “Hackerville” database in MS Access with scrambled password; copy the new encrypted password that is highlighted:



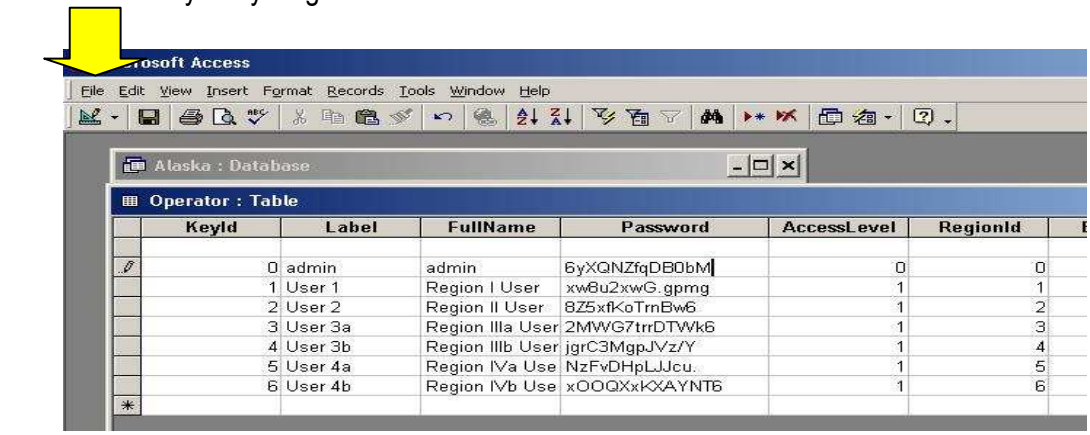
KeyId	Label	FullName	Password	AccessLevel	RegionId	ExportId
0	admin	admin	6yXQNZfqDB0bM	0	0	
2	Auditor John	John R Brakey	v1KUCYsCGPkzk	0	0	
3	Auditor Jim	Jim March	8S3MZEmGkJ/C6	1	0	
4	Auditor Bill	Bill Risner	3KUulLnhX740o	1	0	

18) Paste in the password from Hackerville (in this case “6yXQNZfqDB0bM” which translates from “test”) where “Rptasa4PefgXk” (unknown actual password) is in the Alaska database:

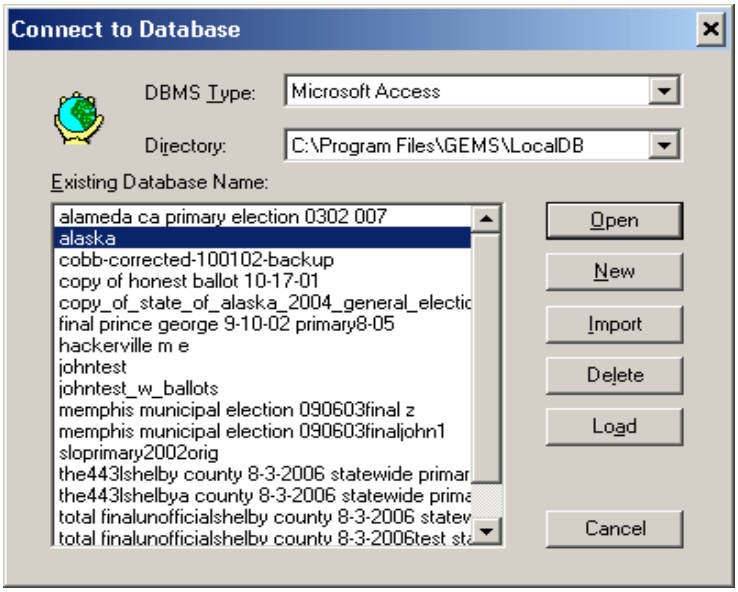
yld	Label	FullNa e	Password	AccessLevel	RegionId
0	admin		Rptasa4PefgXk	0	0
1	User 1		xw8u2xwG.gpmg	1	1
2	User 2	Region II ser	8Z5xfKoTrnBw6	1	2
3	User 3a	Region IIIa User	2MWG7trrDTWk6	1	3
4	User 3b	Region IIIb User	jgrC3MgpJVz/Y	1	4
5	User 4a	Region IVa Use	NzFvDHpLJJcu.	1	5
6	User 4b	Region IVb Use	xOOQXxKXAYNT6	1	6



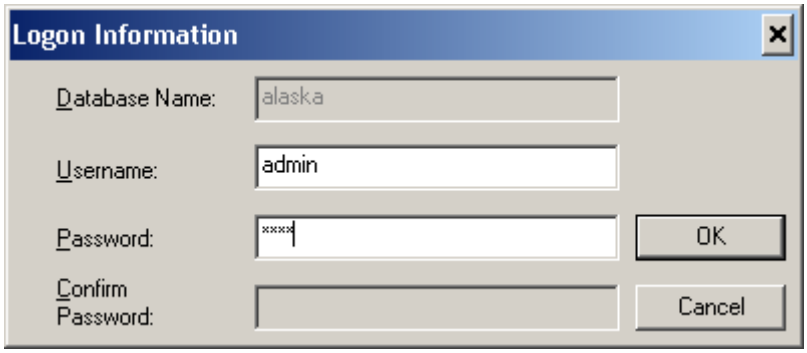
19) Now go to the "file" menu and hit "save" - the new user password (test) will open the Alaska database when you try it again in GEMS.



19) Open the Diebold/GEMS Program:



19) In the password box enter “test” and click “OK”:



20) As you can see below the Election Database is now open using password “test”:

CONCLUSION:

This is just one example of a manipulation of the GEMS data file by way of MS-Access. In reality, every element of the GEMS data (viewed as various tables in MS-Access) can be hand-tweaked. Doing so (in MS-Access) doesn't require a password and doesn't leave any audit trail record AT ALL, even if you don't hand-tune the audit log which is as open to manipulation as anything else.

This demo illustrates why MS-Access has been described as an “election burglary tool”.

However: what is REALLY happening is that a separate program called “Jet” controls the database. Both Access and GEMS control “Jet”. AS CAN MANY OTHER APPLICATIONS, including tiny programs written in “Visual Basic” that would be much harder to spot than the full MS-Access program. Access is the easiest way for non-programmers to hack an election and should therefore be watched for, but the real threat is Diebold's unbelievable design decisions.