Byte Substitutions for Intel Opcodes

In Assembly language, there are many ways of programming the same thing. But did you know that there is also more than one way to program the same opcodes?

The ensuing tables contain the opcodes, followed by 2 sets of bytes which can be used to compile it. The third column is a value which can be XOR'd with the number in one set to produce its counterpart from the other set.

I compiled this list to develop a simple method of substantially changing bytecode in the fewest steps possible. With this method, I not only change the encryption engine itself, but also the bytecode that gets encrypted, by randomly selecting opcode sets to be XORed. I also see the potential of using this concept to "stamp" a binary code with a signature, or perhaps for hiding simple encoded text messages in a functioning executable file. Virus writers will probably find this an interesting method for getting around scan strings.

compiled	set 1	set 2	XOR	compiled	set 1	set 2	XOR
ADC AX,BX	13 C3	11 D8	1B02	ADD AX,BX	03 C3	01 D8	1202
ADC AX,DX	13 C2	11 D0	1202	ADD AX,DX	03 C2	01 D0	1202
ADC BX,AX	13 D8	11 C3	1B02	ADD BX,AX	03 D8	01 C3	1B02
ADC BX,CX	13 D9	11 CB	1202	ADD BX,CX	03 D9	01 CB	1202
ADC CX,BX	13 CB	11 D9	1202	ADD CX,BX	03 CB	01 D9	1202
ADC CX,DX	13 CA	11 D1	1B02	ADD CX,DX	03 CA	01 D1	1B02
ADC DX,AX	13 D0	11 C2	1202	ADD DX,AX	03 D0	01 C2	1202
ADC DX,CX	13 D1	11 CA	1B02	ADD DX,CX	03 D1	01 CA	1B02
ADC SI,AX	13 F0	11 C6	3602	ADD SI,AX	03 F0	01 C6	3602
ADC SI,CX	13 F1	11 CE	3F02	ADD SI,CX	03 F1	01 CE	3F02
ADC DI,AX	13 F8	11 C7	3F02	ADD DI,AX	03 F8	01 C7	3F02
ADC DI,CX	13 F9	11 CF	3602	ADD DI,CX	03 F9	01 CF	3602
ADC AL,BL	12 C3	10 D8	1B02	ADD AL,AL	02 C0	02 C4	400
ADC AL,AL	12 C0	10 D0	1002	ADD AL,BL	00 D8	02 C7	1F02
ADC BL,AL	12 D8	10 C3	1B02	ADD AL,CL	02 C1	02 C5	400
ADC BL,CL	12 D9	10 CB	1202	ADD AL,DL	00 D0	02 C6	1F02
ADC CL,BL	12 CB	10 D9	1202	ADD BL,AL	00 C3	02 DC	400
ADC CL,DL	12 CA	10 D1	1B02	ADD BL,BL	02 DB	02 DF	1602
ADC DL,AL	12 D0	10 C2	1202	ADD BL,CL	00 CB	02 DD	1F02
ADC DL,CL	12 D1	10 CA	1B02	ADD BL,DL	02 DA	02 DE	400
ADC AH,BL	12 E3	10 DC	3F02	ADD CL,AL	02 C8	02 CC	400
ADC AH,DL	12 E2	10 D4	3602	ADD CL,BL	00 D9	02 CF	1602
ADC BH,AL	12 F8	10 C7	3F02	ADD CL,CL	02 C9	02 CD	400
ADC BH,CL	12 F9	10 CF	3602	ADD CL,DL	00 D1	02 CA	1B02
ADC CH,BL	12 EB	10 DD	3602	ADD DL,AL	00 C2	02 D4	1602
ADC CH,DL	12 EA	10 D5	3F02	ADD DL,BL	02 D3	02 D7	400
ADC DH,AL	12 F0	10 C6	3602	ADD DL,CL	00 CA	02 D5	1F02
ADC DH,CL	12 F1	10 CE	3F02	ADD DL,DL	02 D2	02 D6	400
ADC AH,BH	12 E7	10 FC	1B02	ADD AH,BL	00 DC	02 E3	3F02
ADC AH,DH	12 E6	10 F4	1202	ADD AH,DL	00 D4	02 E2	3606
ADC BH,AH	12 FC	10 E7	1B02	ADD BH,AL	00 C7	02 F8	3F02
ADC BH,CH	12 FD	10 EF	1202	ADD BH,CL	00 CF	02 F9	3602
ADC CH,BH	12 EF	10 FD	1202	ADD CH,AL	00 DD	02 EB	3602
ADC CH,DH	12 EE	10 F5	1B02	ADD CH,CL	00 D5	02 EA	3F02
ADC DH,AH	12 F4	10 E6	1202	ADD DH,AL	00 C6	02 F0	3602
ADC DH,CH	12 F5	10 EE	1B02	ADD DH,CL	00 CE	02 F1	3F02

ADC AL,BH	12 F8	10 F8	2		ADD AH,BH	00 FC	02 E7	1B02
ADC AL,DH	12 F0	10 F0	2		ADD AH,DH	00 F4	02 E6	1202
ADC BL,AH	12 E3	10 E3	2		ADD BH,AH	00 E7	02 FC	1B02
ADC BL,CH	12 EB	10 EB	2		ADD BH,CH	00 EF	02 FD	1202
ADC CL,BH	12 F9	10 F9	2		ADD CH,BH	00 FD	02 EF	1202
ADC CL,CH	12 F1	10 F1	2		ADD CH,DH	00 F5	02 EE	1B02
ADC DL,AH	12 E2	10 E2	2		ADD DH,AH	00 E6	02 F4	1202
ADC DL,CH	12 EA	10 EA	2		ADD DH,CH	00 EE	02 F5	1B02
ADC AX,SI	13 C6	11 F0	C902		ADD AL,BH	00 F8	02 C7	3F02
ADC CX,SI	13 CE	11 F1	3F02		ADD AL,DH	00 F0	02 C6	3602
ADC AX,DI	13 C7	11 F8	3F02		ADD BL,AH	00 E3	02 DC	3F02
ADC CX,DI	13 CF	11 F9	3602		ADD BL,CH	00 EB	02 DD	3602
					ADD CL,BH	00 F9	02 CF	3602
					ADD CL,DH	00 F1	02 CE	3F02
					ADD DL,AH	00 E2	02 D4	3602
					ADD DL,CH	00 EA	02 D5	3F02
					ADD AX,SI	01 F0	03 C6	3602
					ADD CX,SI	01 F1	03 CE	3F02
					ADD AX,DI	01 F8	03 C7	3F02
					ADD CX,DI	01 F9	03 CF	3602
AND AX,BX	23 C3	21 D8	1B02		CMP AX,BX	3B C3	39 D8	1B02
AND AX,DX	23 C2	21 D0	1202		CMP AX,DX	3B C2	39 D0	1202
AND BX,AX	23 D8	21 C3	1B02		CMP BX,AX	3B D8	39 C3	1B02
AND BX,CX	23 D9	21 CB	1202		CMP BX,CX	3B D9	39 CB	1202
AND CX,BX	23 CB	21 D9	1202		CMP CX,BX	3B CB	39 D9	1202
AND CX,DX	23 CA	21 D1	1B02		CMP CX,DX	3B CA	39 D1	1B02
AND DX,AX	23 D0	21 C2	1202		CMP DX,AX	3B D0	39 C2	1202
AND DX,CX	23 D1	21 CA	1B02		CMP DX,CX	3B D1	39 CA	1B02
AND SI,AX	23 F0	21 C6	3602		CMP SI,AX	3B F0	39 C6	3602
AND SI,CX	23 F1	21 CE	3F02		CMP SI,CX	3B F1	39 CE	3F02
AND DI,AX	23 F8	21 C7	3F02		CMP DI,AX	3B F8	39 C7	3F02
AND DI,CX	23 F9	21 CF	3602		CMP DI,CX	3B F9	39 CF	3602
AND AX,SI	23 C6	21 F0	3602		CMP AX,SI	3B C6	39 F0	3602
AND CX,SI	23 CE	21 F1	3F02		CMP CX,SI	3B CE	39 F1	3F02
AND AX,DI	23 C7	21 F8	3F02		CMP AX,DI	3B C7	39 F8	3F02
AND CX,DI	23 CF	21 F9	3602		CMP CX,DI	3B CF	39 F9	3602
MOV AX,AX	8B C0	89 C0	2		OR AX,BX	0B C3	09 D8	1B02
MOV AX,CX	8B C1	89 C8	902		OR AX,DX	0B C2	09 D6	1402
MOV BX,BX	8B DB	89 DB	2		OR AX,SI	0B C6	09 F0	3602
MOV BX,DX	8B DA	89 D3	902		OR AX,DI	0B C7	09 F8	3F02
MOV BX,SI	8B DE	89 F3	2D02		OR BX,AX	0B D8	09 C3	1B02
MOV BX,DI	8B DF	89 FB	2402		OR BX,CX	0B D9	09 CB	1202
MOV CX,AX	8B C8	89 C1	902		OR CX,BX	0B CB	09 D9	1202
MOV CX,CX	8B C9	89 C9	2		OR CX,DX	0B CA	09 D1	1B02
MOV DX,BX	8B D3	89 DA	902		OR CX,SI	0B DE	09 F1	2F02
MOV DX,DX	8B D2	89 D2	2		OR CX,DI	0B CF	09 F9	3602
MOV DX,SI	8B D6	89 F2	2402		OR DX,AX	0B D0	09 C2	1202
MOV DX,DI	8B D7	89 FA	2D02		OR DX,CX	0B D1	09 CA	1B02
MOV SI,BX	8B F3	89 DE	2D02		OR SI,AX	0B F0	09 C6	3602
MOV SI,DX	8B F2	89 D6	2402		OR SI,CX	0B F1	09 CE	3F02
MOV SI,SI	8B F6	89 F6	2		OR DI,AX	0B F8	09 C7	3F02
MOV SI,DI	8B F7	89 FE	902		OR DI,CX	0B F9	09 CF	3602
MOV DI,BX	8B FB	89 DF	2402		OR AL,BL	0A C3	08 D8	1B02
MOV DI,DX	8B FA	89 D7	2D02		OR AL,DL	0A C2	08 D0	1202
MOV DI,SI	8B FE	89 F7	902		OR BL,AL	0A D8	08 C3	1B02
MOV DI,DI	8B FF	89 FF	2		OR BL,CL	0A D9	08 CB	1202
MOV AL,AL	8A C0	88 C0	2		OR CL,BL	0A CB	08 D9	1202
MOV AL,CL	8A C1	88 C8	902		OR CL,DL	0A CA	08 D1	1B02
MOV BL,DL	8A DA	88 D3	902		OR DL,AL	0A D0	08 C2	1202

MOV CL,AL	8A C8	88 C1	902		OR DL,CL	0A D1	08 CA	1B02
MOV CL,CL	8A C9	88 C9	2		OR AH,BL	0A E3	08 DC	3F02
MOV DL,BL	8A DA	88 DA	2		OR AH,DL	0A E2	08 D4	3602
MOV DL,DL	8A D2	88 D2	2		OR BH,AL	0A F8	08 C7	3F02
MOV AH,AL	8A E0	88 C4	2402		OR BH,CL	0A F9	08 CF	3602
MOV AH,CL	8A E1	88 CC	2D02		OR CH,BL	0A EB	08 DD	3602
MOV BH,BL	8A FB	88 DF	2402		OR CH,DL	0A EA	08 D5	3F02
MOV BH,DL	8A FA	88 D7	2D02		OR DH,AL	0A F0	08 C6	3602
MOV CH,AL	8A E8	88 C5			OR DH,CL	0A F1	08 CE	
MOV CH,CL	8A E9	88 CD			OR AH,BH	0A E7	08 FC	
MOV DH,BL	8A F3	88 DE			OR AH,DH	0A E6	08 F4	
MOV DH,DL	8A F2	88 D6			OR BH,AH	0A FC	08 E7	
MOV AH,CH	8A E5	88 EC			OR BH,CH	0A FD	08 EF	
MOV BH,BH	8A FF	88 FF			OR CH,BH	0A EF	08 FD	
MOV BH,DH	8A FE	88 F7			OR CH,DH	0A EE	08 F5	
MOV CH,AH	8A EC	88 E5			OR DH,AH	0A F4	08 E6	
MOV DH,DH	8A F6	88 F6			OR DH,CH	0A F5	08 EE	
MOV AL,AH	8A C4	88 E0			OR AL,BH	0A C7	08 F8	
MOV AL,CH	8A C5	88 E8			OR AL,DH	0A C6	08 F0	
MOV BL,BH	8A DF	88 FB			OR BL,AH	0A DC	08 E3	
MOV BL,DH	8A DE	88 F3			OR BL,CH	0A DD	08 EB	
MOV CL,AH	8A CC	88 E1			OR CL,BH	0A CF	08 F9	
MOV CL,CH	8A CD	88 E9			OR CL,DH	0A CE	08 F1	
MOV DL,BH	8A D7	88 FA			OR DL,AH	0A D4	08 E2	
MOV DL,DH	8A D6	88 F2			OR DL,CH	0A D5	08 EA	

SBB AX,BX	1B C3	19 D8			SUB AX,BX	2B C3	29 D8	
SBB AX,DX	1B C2	19 D6			SUB AX,DX	2B C2	29 D6	
SBB AX,SI	1B C6	19 F0			SUB AX,SI	2B C6	29 F0	
SBB AX,DI	1B C7	19 F8			SUB AX,DI	2B C7	29 F8	
SBB BX,AX	1B D8	19 C3			SUB BX,AX	2B D8	29 C3	
SBB BX,CX	1B D9	19 CB			SUB BX,CX	2B D9	29 CB	
SBB CX,BX	1B CB	19 D9			SUB CX,BX	2B CB	29 D9	
SBB CX,DX	1B CA	19 D1			SUB CX,DX	2B CA	29 D1	
SBB CX,SI	1B DE	19 F1			SUB CX,SI	2B DE	29 F1	
SBB CX,DI	1B CF	19 F9			SUB CX,DI	2B CF	29 F9	
SBB DX,AX	1B D0	19 C2			SUB DX,AX	2B D0	29 C2	
SBB DX,CX	1B D1	19 CA			SUB DX,CX	2B D1	29 CA	
SBB SI,AX	1B F0	19 C6			SUB SI,AX	2B F0	29 C6	
SBB SI,CX	1B F1	19 CE			SUB SI,CX	2B F1	29 CE	
SBB DI,AX	1B F8	19 C7			SUB DI,AX	2B F8	29 C7	
SBB DI,CX	1B F9	19 CF			SUB DI,CX	2B F9	29 CF	
SBB AL,BH	1A C7	18 F8			SUB AL,BL	2A C3	28 D8	
SBB AL,DH	1A C6	18 F0			SUB AL,DL	2A C2	28 D0	
SBB BL,AH	1A DC	18 E3			SUB BL,AL	2A D8	28 C3	
SBB BL,CH	1A DD	18 EB			SUB BL,CL	2A D9	28 CB	
SBB CL,BH	1A CF	18 F9			SUB CL,BL	2A CB	28 D9	
SBB CL,DH	1A CE	18 F1			SUB CL,DL	2A CA	28 D1	
SBB DL,AH	1A D4	18 E2			SUB DL,AL	2A D0	28 C2	
SBB DL,CH	1A D5	18 EA			SUB DL,CL	2A D1	28 CA	
SBB AL,BL	1A C3	18 D8			SUB AL,BH	2A C7	28 F8	
SBB AL,DL	1A C2	18 D0			SUB AL,DH	2A C6	28 F0	
SBB BL,AL	1A D8	18 C3			SUB BL,AH	2A DC	28 E3	
SBB BL,CL	1A D9	18 CB			SUB BL,CH	2A DD	28 EB	
SBB CL,BL	1A CB	18 D9			SUB CL,BH	2A CF	28 F9	
SBB CL,CL	1A CA	18 D1			SUB CL,DH	2A CE	28 F1	
SBB DL,AL	1A D3	18 C2			SUB DL,AH	2A D4	28 E2	
SBB DL,CL	1A D1	18 CA			SUB DL,CH	2A D5	28 EA	
SBB AH,BL	1A E3	18 DC			SUB AH,BH	2A E7	28 FC	
SBB AH,DL	1A E2	18 D4			SUB AH,DH	2A E6	28 F4	
SBB BH,AL	1A F8	18 C7			SUB BH,AH	2A FC	28 E7	

SBB BH,CL	1A F9	18 CF
SBB CH,BL	1A EB	18 DD
SBB CH,DL	1A EA	18 D5
SBB DH,AL	1A F0	18 C6
SBB DH,CL	1A F1	18 CE
SBB AH,BH	1A E7	18 FC
SBB AH,CH	1A E6	18 F4
SBB BH,AH	1A FC	18 E7
SBB BH,CH	1A FD	18 EF
SBB CH,BH	1A EF	18 FD
SBB CH,DH	1A EE	18 F5
SBB DH,AH	1A F4	18 E6
SBB DH,CH	1A F5	18 EE

XOR AL,BL	32 C3	30 D8
XOR AL,DL	32 C2	30 D0
XOR BL,AL	32 D8	30 C3
XOR BL,CL	32 D9	30 CB
XOR CL,BL	32 CB	30 D9
XOR CL,DL	32 CA	30 D1
XOR DL,AL	32 D0	30 C2
XOR DL,CL	32 D1	30 CA
XOR AH,BL	32 E3	30 DC
XOR AH,DL	32 E2	30 D4
XOR BH,AL	32 F8	30 C7
XOR BH,CL	32 F9	30 CF
XOR CH,BL	32 EB	30 DD
XOR CH,DL	32 EA	30 D5
XOR DH,AL	32 FD	30 C6
XOR DH,CL	32 F1	30 CE
XOR AH,BH	32 E7	30 FC
XOR AH,DH	32 E6	30 F4
XOR BH,AH	32 FC	30 E7
XOR BH,CH	32 FD	30 EF
XOR CH,BH	32 EF	30 FD
XOR CH,DH	32 EE	30 F5
XOR DH,AH	32 F4	30 E6
XOR DH,CH	32 F5	30 EE
XOR AL,BH	32 C7	30 F8
XOR AL,DH	32 C6	30 F0
XOR BL,AH	32 DC	30 E3
XOR BL,CH	32 DD	30 EB
XOR CL,BH	32 CF	30 F9
XOR CL,DH	32 CE	30 F1
XOR DL,AH	32 D4	30 E2
XOR DL,CH	32 D5	30 EA

SUB BH,CH	2A FD	28 EF
SUB CH,BH	2A EF	28 FD
SUB CH,DH	2A EE	28 F5
SUB DH,AH	2A F4	28 E6
SUB DH,CH	2A F5	28 EE
SUB AH,BL	2A E3	28 DC
SUB AH,DL	2A E2	28 D4
SUB BH,AL	2A F8	28 C7
SUB BH,CL	2A F9	28 CF
SUB CH,BL	2A EB	28 DD
SUB CH,DL	2A EA	28 D5
SUB DH,AL	2A F0	28 C6
SUB DH,CL	2A F1	28 CE

XOR AX,BX	33 C3	31 D8
XOR AX,DX	33 C2	31 D0
XOR AX,SI	33 C6	31 F0
XOR BX,CX	33 D9	31 CB
XOR CX,BX	33 CB	31 D9
XOR CX,DX	33 CA	31 D1
XOR CX,SI	33 CE	31 F1
XOR CX,DI	33 CF	31 F9
XOR DX,AX	33 D0	31 C2
XOR DX,CX	33 D1	31 CA
XOR SI,AX	33 F0	31 C6
XOR SI,CX	33 F1	31 CE
XOR DI,AX	33 F8	31 C7
XOR DI,CX	33 F9	31 CF
XOR AX,DI	33 CF	31 F8