

الفريق العربي للهندسة الميكانيكية

دورة ATRE لتعليم الأسهل للمبتدئين من الصفر
الدرس الثاني — مفهوم جهاز الكمبيوتر – مكونات المعالج

جهاز الكمبيوتر هو آلة كهربائية تأخذ البيانات والتعليمات (*inputs*) ، ثم تقوم بمعالجتها (*processing*) ، وتخرج لنا المخرجات (*outputs*) .
جهاز الكمبيوتر مر بخمسة أجيال كل جيل كان له خصائص معينة... (لمزيد من التفاصيل www.google.com) .
كما و يقسم الكمبيوتر إلى عدة أقسام (Ranges) منها :

- embedded system computer (e.g. : washing machine)
- microcomputers
- minicomputers
- mainframe computers
- super computers

جهاز الحاسوب الذي أمامك ينتمي إلى الجيل الخامس ، وإلى قسم الثاني.
يتكون جهاز الحاسوب من 5 أقسام أساسية :

I -central processing unit (CPU)

II -input devices

III-memory storage devices

IV-output devices

V -a communication network , called "bus" , that links all the elements of the system and connects the system to the external world.

وحدة المعالجة المركزية : Central Processing Unit (CPU)

ال CPU قد تكون شريحة (chip) مفردة أو عدة شرائح متصلة مع بعضها البعض حيث تقوم بتنفيذ العمليات الحسابية والمنطقية (arithmetic and logical calculations) وتقوم بتنظيم تزامن العمليات الأخرى في الحاسوب والتحكم بها. مع تطور التكنولوجيا ظهر ما يسمى بال microprocessor الذي يتضمن المزيد من الدوائر الكهربائية والذاكرة داخليا. والنتيجة جهاز حاسوب بحجم أصغر بكثير...
معظم ال CPU تتكون من المكونات الأساسية التالية :

- arithmetic logic unit (ALU)
- registers
- control section
- internal bus

أولا - وحدة الحساب والمنطق (Arithmetic Logical Unit (ALU)

هذه الوحدة مسئولة عن العمليات الحسابية (جمع طرح ...) والمنطقية (or , xor , and , etc...) وعمليات المقارنة بين البيانات (أكبر أصغر...).

ثانيا - المسجلات Registers

إن ال CPU يحتوي على وحدات ذاكرة صغيرة لكن سريعة جدا تستخدم لعمليات التخزين المؤقتة (temporary) للبيانات. هذه الذاكرة تحتوي على عدد من المسجلات registers ، كل واحدة تقوم بعملية محددة... وسيلي شرح تفصيلي عن المسجلات لاحقا.

ثالثا - وحدة التحكم (CU) Control Unit

إن العمليات التي يتم تنفيذها من قبل ال CPU هي بالتسلسل التالي :

1- فك تشفير التعليمات

within the computer. decoding the instruction

2- تنظيم تزامن عمليات القراءة والكتابة بداخل ال CPU وخارجيا في ممرات البيانات

Sequencing the reading and writing of data within the CPU and externally on the Data Bus.

3- التحكم في التزامن الذي يتم من خلاله تنفيذ العمليات

Controlling the sequence in which instructions are executed.

4- التحكم بالعمليات التي يتم تنفيذها من قبل ال ALU

Controlling the operations performed by the ALU.

رابعا - الممر الداخلي Internal Bus

هو عبارة عن شبكة من أسلاك الاتصالات التي تربط العناصر الداخلية للمعالج ببعضها البعض ، وأيضا تؤدي إلى اتصالات خارجية تربط المعالج بالعناصر الأخرى للنظام - أي للكمبيوتر .

هناك ثلاث أنواع من ال CPU Buses :

Control Bus-1 : يتكون من الخط (line) الذي يستشعر (senses) الإشارات الداخلية بالإضافة إلى خطوط أخرى للتحكم بالإشارات بداخل ال CPU .

2- The address Bus ، خط باتجاه واحد من المعالج الذي يحوي عناوين الذاكرة للبيانات .

3- the Data Bus ، خط باتجاهين يقوم بقراءة البيانات من الذاكرة وكتابتها إليها .

نظرة تاريخية على المعالجات...

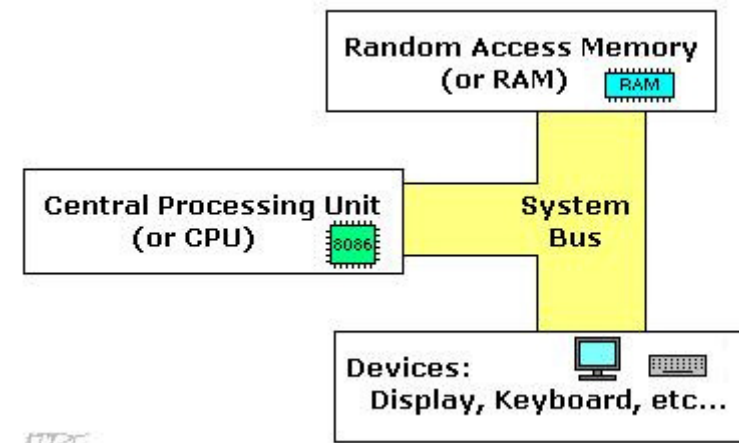
في السبعينيات طرحت شركة انتل معالج 4004 وهو أول μP من نوع single-chip... وعندما نقول أنه 4-bit فنحن نعني أن ال Bus Width يساوي 4 bit . كان قادرا على عنوان ذاكرة حتى حجم 640 بايت فقط. تلا هذا الطراز عدة طرازات... ثم جاء ال 8086 في سنة 1978 وبنقل بيانات ال Bus باتساع 16-Bit... وبنقل عناوين ال bus addresses باتساع 20 بت. كان قادرا على عنوان ذاكرة حتى حجم 1 ميجابايت... تلا ذلك عدة أنواع وموديلات أصبحت مزودة بنقل بيانات باتساع 32 بت ، وهو ال Pentium ، وأيضا صدرت بعض المعالجات بنقل بيانات باتساع 64 بت ك titanium ، للإطلاع على قائمة بجميع الموديلات وتفاصيلها زر هذه الصفحة :

http://en.wikipedia.org/wiki/List_of_Intel_microprocessors

إن معالجي 8086 و 8088 متشابهين كثيرا من حيث الخصائص... وهذا السبب الذي يدفعنا لتسميتهم باسم ...x-86 family

لغة الأسمبلي... ما هي ؟

هي لغة برمجة منخفضة المستوى (low level) ، كي تيرمج الأسمبلي يلزمك معرفة بال computer structure ، يمكننا توضيح ال computer model كالتالي :



والآن دعنا نلقي نظرة مفصلة على المسجلات التي بداخل ال CPU ...
(ملاحظة : لن أنطرق إلى ال internal architecture للمعالج... سأكتفي بما يهمنا بطريقة مباشرة فقط)

31	16	15	8	7	0
EAX	AH	AL			
EBX	BH	BL			
ECX	CH	CL			
EDX	DH	DL			
ESI	SI				
EDI	DI				
ESP	SP				
EBP	BP				

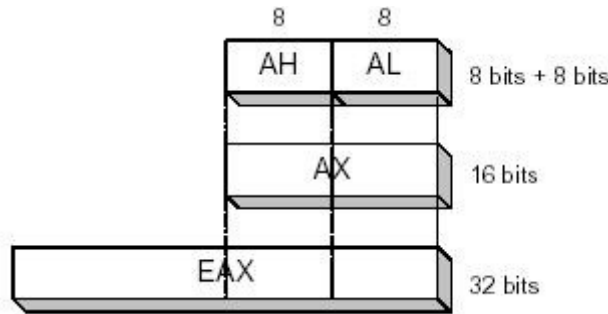
CS
SS
DS
ES
FS
GS
IP

كما ترى هناك في هذا المخطط عدة أقسام للمسجلات...
: **general purpose registers**

إن معالجات 8086 تمتلك 8 مسجلات عامة الغرض ، ولكل منها اسم خاص :

- **EAX** - the accumulator register.
- **EBX** - the base address register.
- **ECX** - the count register
- **EDX** - the data register
- **ESI** - source index register.
- **EDI** - destination index register.
- **EBP** - base pointer.
- **ESP** - stack pointer.

الواقع فإن تلك المسجلات الأربع : EAX ,EBX,ECX,EDX لها التركيب التالي :



عند التعامل مع هذه المسجلات يمكنك الوصول إلى الـ 32 بت عن طريق EAX أو إلى أول 16 بت عن طريق AX أو حتى إلى أول وثنائي 8 بت عن طريق AL و AH على الترتيب. لاحظ أن القسم العلوي من EAX لا يمكن الوصول إليه على انفراد. فقط القسم السفلي يمكنك التعامل معه بشكل منفرد . طبعاً ما ينطبق على EAX ينطبق على EBX,ECX,EDX .

على الرغم من التسمية لكل مسجل ، فإن المبرمج هو الذي يحدد استخدامات كل مسجل منها...
جدير بالذكر أن التعامل مع هذه الذاكر يتم بكل سرعة لأنها موجودة بداخل المعالج بعكس الذاكرة RAM (أو غيرها) حيث التعامل معها يتطلب استخدام الـ Buses مما يسبب تأخيراً زمنياً...

: **segment registers**

- CS - points at the segment containing the current program.
- DS - generally points at segment where variables are defined.
- ES - extra segment register, it's up to a coder to define its usage.
- SS - points at the segment containing the stack.

أيضاً هناك مسجلين إضافيين في المعالجات الحديثة (نسبياً) هما FS و GS .
على الرغم من أنه يمكنك تخزين أي قيمة في الـ segment registers ، فإن هذه لم ولن تكون فكرة صائبة... لأن هذا النوع من المسجلات ليس عام الغرض ، بل له مهمة محددة وهي pointing at accessible blocks of memory (لا تسألني عن الترجمة :).

إن ال segment registers تعملان جنباً إلى جنب مع ال general purpose registers للوصول إلى أي عنوان ذاكرة.

على سبيل المثال إذا أردنا الوصول إلى عنوان الذاكرة الفيزيائي 12345h يجب أن نضع DS = 1230h و SI = 0045h . هذه طريقة جيدة لأنه هكذا يمكننا الوصول إلى عدد أكبر من العناوين بدلا من التقيد بالـ 16 بت التي تملكها ال segment registers .
إن ال CPU يقوم بعمليات حسابات للعنوان الفيزيائي بضرب ال segment register بـ 10h وجمعه مع ال general purpose register . هكذا :

$$\begin{array}{r} 12300 \\ + 0045 \\ \hline 12345 \end{array}$$

إن العنوان المكون بمسجلين إثنين يسمى effective address . بشكل افتراضي ، فإن BX, SI and DI تعمل مع DS أما BP and SP فتعمل مع SS .
المسجلات العامة الغرض الأخرى لا يمكنها أن تكون effective address .

: special purpose registers

- EIP the instruction pointer.
- flags register - determines the current state of the microprocessor.

إن EIP دائما يعمل مع CS ، وهو يشير دائما وأبدا إلى التعليمة التي يجري تنفيذها حاليا.

الرايات : Flag registers

إن الرايات يتم تغييرها تلقائيا من قبل ال CPU بعد تنفيذ عمليات رياضية ومنطقية . إنها تسمح بمعرفة نتيجة العملية وتحديد الشروط لنقل التحكم إلى أجزاء أخرى من البرنامج .
بشكل عام لا يمكنك تغيير قيم هذه المسجلات بطريقة مباشرة...هناك طرق غير مباشرة قد تأتي على ذكرها في دروس قادمة...

31	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reserved	AG	VM	RF	0	NT	IOPL	O	D	I	T	S	Z	A	P	C				

تقسم الرايات إلى ثلاثة أقسام: (مع الشكر للأخ afeef على دروسه حيث نسخت التالي كما هو :)
- **رايات غير مستعملة** أي أنها لا تفيد في الحكم على آخر عملية وهي موجودة فقط في حالة تطوير المعالج ربما يحتاجون إلى رايات إضافية فيمكن استغلال هذه الرايات. في الوقت الحالي نحن لسنا بحاجة إليها
- **رايات الوضع**: وهي الرايات التي تتأثر وتتغير حسب وضع العمليات التي تقوم بها وحدة الحساب والمنطق في المعالج
- **رايات السيطرة**: وهي رايات المبرمج يتحكم بوضعها فإذا وضع بداخلها القيمة 1 تبقى هذه القيمة حتى يغيرها المبرمج في البرنامج عن طريق أوامر برمجة خاصة بها

مسجل الرايات في المعالج 8086 يحتوي على 7 رايات غير مستخدمة 6 رايات وضع و 3 رايات سيطرة

CF	Carry flag
PF	Parity flag
AF	Auxiliary flag
ZF	Zero flag
SF	Sign flag
TF	Trap flag
IF	Interrupt flag
DF	Direction Flag
OF	Overflow flag

إلى هنا يكون درس اليوم قد انتهى... لا يوجد assignment لهذا الدرس... أراكم في الدرس القادم

References:

- 1- <http://www.emu8086.com/>
- 2- Assembly Language for Intel-Based Computers , Kip. R. Irvine
- 3- Fundamentals of Computer Organization and Architecture ,
Mostafa Abd-El-Barr and Hesham El-Rewini.
- 4- <http://www.arabteam2000.com/>

Arab Team for Reverse Engineering

αλλκο
July - 2006