Hamiltonion Circuit is **NP**-complete

HC is in **NP**:
To see that HC is in **NP** consider the following machine M. Suppose a graph G=(V,E) is given. Guess a permutation $v_1v_2\ldots v_n$ and check that $v_1v_2\ldots v_nv_1$ is indeed a circuit in the graph.

HC is **NP**-hard:
We show that VC $\leq_m^p$ HC
Suppose $G = (V, E)$, along with a number K, is the given VC problem.
We construct a graph (V', E') as follows.

For each edge $e = (u, v) \in E$, we have 12 vertices:
$V'_e = \{[u, e, i], [v, e, i] : 1 \leq i \leq 6\}$
along with the edges
$E'_e = \{([u, e, i], [u, e, i + 1]) : 1 \leq i \leq 5\} \cup$
$\{([v, e, i], [v, e, i + 1]) : 1 \leq i \leq 5\} \cup$
$\{([u, e, 1], [v, e, 3]), ([u, e, 4], [v, e, 6]),$
$([v, e, 1], [u, e, 3]), ([v, e, 4], [u, e, 6])\ \}$

For each vertex $v \in V$, we have the edges
$E'_v = \{([v, e_{v(j)}, 6], [v, e_{v(j+1)}, 1]) : 1 \leq j < deg(v)\}$
where $e_{v(1)}, e_{v(2)}, \ldots, e_{deg(v)}$ are the edges with one end-point being v.

Special vertices and edges:

$V'' = \{a_i : 1 \leq i \leq K\}$

$E'' = \{(a_i, [v, e_{v(1)}, 1]), ([v, e_{v(deg(v))}, 6], a_i) : 1 \leq i \leq K, v \in V\}$

$V' = V'' \cup \left(\cup_{e \in E} V'_e\right)$

$E' = E'' \cup \left(\cup_{e \in E} E'_e\right) \cup \left(\cup_{v \in V} E'_v\right).$

Why does it work?

Sketch:

For each edge, consider the portion of the graph:

V'_e and E'_e.

Note that the vertices $[u, e, i], [v, e, i]$, for $2 \leq i \leq 5$ do not appear in any other edge in E'. Thus, in the Hamiltonian circuit, these vertices must be covered only using the edges in E'_e. This can only be done in one of three ways as follows:

First way: $([u, e, 1], [u, e, 2], [u, e, 3], [u, e, 4], [u, e, 5], [u, e, 6])$ and $([v, e, 1], [v, e, 2], [v, e, 3], [v, e, 4], [v, e, 5], [v, e, 6])$ are part of the HC.

Second way: $([u, e, 1], [u, e, 2], [u, e, 3], [v, e, 1], [v, e, 2], [v, e, 3], [v, e, 4], [v, e, 5], [v, e, 6], [u, e, 4], [u, e, 5], [u, e, 6])$, is a part of the HC.

Third way: $([v, e, 1], [v, e, 2], [v, e, 3], [u, e, 1], [u, e, 2], [u, e, 3], [u, e, 4], [u, e, 5], [u, e, 6], [v, e, 4], [v, e, 5], [v, e, 6])$, is a part of the HC.

Note that in all the above cases, if the HC enters using vertex $[u, e, 1]$, then it exits via the vertex $[u, e, 6]$, and if it enters using vertex $[v, e, 1]$, then it exits via the vertex $[v, e, 6]$.
The only edges which connect $[u, e, 1], [u, e, 6]$ to the other vertices of the graph G' are from E'_u and E''.
In particular, this means that if the HC uses first or second way for some edge e incident on vertex u, (we call this way of covering V_e as V_e is covered using u), then for every edge e' incident on vertex u, we must have that $V_{e'}$ is covered using u.
Thus, one can intuitively think of the first way as the vertex cover containing both u and v, second way as the vertex cover containing u (but not v) and the third way as the vertex cover containing v (but not u).
Also note that if we cover V_e using u, then in the HC, the coverage of $V_{e'}$, e' is incident on u, are all linked one after another.

Suppose the graph G has a vertex cover of size $\leq k$. Without loss of generality assume the vertex cover S is of size exactly k.
Then, the HC is formed as follows.
Order the k vertices in S in some way, say $v_1, v_2, \ldots, v_k$.
Form the HC by using

a_1,
$[v_1, e_{v_1(1)}, 1], \ldots [v_1, e_{v_1(1)}, 6], [v_1, e_{v_1(2)}, 1], [v_1, e_{v_1(2)}, 6], \ldots,$
$[v_1, e_{v_1(deg(v_1))}, 1], \ldots, [v_1, e_{v_1(deg(v_1))}, 6],$
a_2,
$[v_2, e_{v_2(1)}, 1], \ldots [v_2, e_{v_2(1)}, 6], [v_2, e_{v_2(2)}, 1], [v_2, e_{v_2(2)}, 6], \ldots,$
$[v_2, e_{v_2(deg(v_2))}, 1], \ldots, [v_2, e_{v_2(deg(v_2))}, 6],$
$\ldots,$
a_k,
$[v_k, e_{v_k(1)}, 1], \ldots [v_k, e_{v_k(1)}, 6], [v_k, e_{v_k(2)}, 1], [v_k, e_{v_k(2)}, 6], \ldots,$
$[v_k, e_{v_k(deg(v_k))}, 1], \ldots, [v_k, e_{v_k(deg(v_k))}, 6],$
a_1

Suppose there is a HC in G'

Without loss of generality assume that the HC starts at a_1, then goes via a_2, a_3, $\ldots$, a_k and back to a_1, where the other vertices are covered in the intermediate steps between these a_i's. (If there is some other order of covering the a_i's, one can just rename the a_i's). Now, between a_i and a_{i+1} there must be a "chain" using some vertex, say v_i. Similary, between a_k and a_1, there must be a chain using some vertex v_k. Then one selects $v_1, v_2, \ldots, v_k$ as the vertex cover. Details of verification that above works is left as an exercise.