Sécurité, identification usager, droits et chiffrement

Question 1

Vous consulterez la vue dba users pour constater que vous avez effectivement accès à l'image MD5 de chaque mot de passe utilisateur. Quels sont les dispositifs qui pourraient mettre à mal la protection associée à cette clé de hachage ? Quels sont les moyens pour limiter le risque de "piratage" des mots de passe ?

```
select username,password from dba_users;
```

Ne fonctionne pas à la fac, mot de passe vide.

Solutions :

- Utiliser des mots de passe suffisament longs
- Utilser un autre élement associé à l'utilisateur au mot de passe pour crypter

Question 2

Quelles sont les vues à consulter pour connaître les utilisateurs qui disposent du plus grand nombre de droits sur la base de données ? Proposer des requêtes adaptées à la consultation de ces droits (nom utilisateur, catégories de droits) ?

```
select * from dba_role_privs;
```

GRANTEE	GRANTED_ROLE	ADM	DEF
NROUCH02	CONNECT	NO	YES
DKULCZYNSKI	SELECT_CATALOG_ROLE	NO	YES
KCHAZALON	RESOURCE	NO	YES
MDIALLO02	CONNECT	NO	YES
HALHOUSSEINI	SELECT_CATALOG_ROLE	NO	YES
WDURAND	RESOURCE	NO	YES
ASORIANO	RESOURCE	NO	YES
KCHALLAL	SELECT_CATALOG_ROLE	NO	YES
NDECHACHE	RESOURCE	NO	YES
NDECHACHE	SELECT_CATALOG_ROLE	NO	YES
ABENSEDRINE	CONNECT	NO	YES

```
select * from dba_sys_privs;
```

GRANTEE	PRIVILEGE	ADM
AHADDADJ	DROP ANY MATERIALIZED VIEW	NO
NGILBERT	CREATE ANY VIEW	NO
NGILBERT	CREATE PUBLIC DATABASE LINK	NO
MDULONDEL	CREATE ANY MATERIALIZED VIEW	NO
LATOUI	DROP ANY MATERIALIZED VIEW	NO
ATURPAULT	CREATE PUBLIC DATABASE LINK	NO
KSUGIER	DROP ANY MATERIALIZED VIEW	NO
KCHALLAL	DROP ANY MATERIALIZED VIEW	NO
ABARRAY	DROP PUBLIC DATABASE LINK	NO
ABARRAY	CREATE ANY MATERIALIZED VIEW	NO
FKROMAH	DROP ANY MATERIALIZED VIEW	NO

```
select grantee,owner,table_name,privilege from dba_tab_privs;
```

GRANTEE	OWNER	TABLE_NAME	PRIVILEGE
PUBLIC	WMSYS	ALL_VERSION_HVIEW_WDEPTH	SELECT
PUBLIC	WMSYS	ALL_WM_CONSTRAINTS	SELECT
PUBLIC	WMSYS	ALL_WM_CONS_COLUMNS	SELECT
PUBLIC	WMSYS	ALL_WM_IND_COLUMNS	SELECT
PUBLIC	WMSYS	ALL_WM_IND_EXPRESSIONS	SELECT
PUBLIC	WMSYS	ALL_WM_LOCKED_TABLES	SELECT
PUBLIC	WMSYS	ALL_WM_MODIFIED_TABLES	SELECT
PUBLIC	WMSYS	ALL_WM_RIC_INFO	SELECT
PUBLIC	WMSYS	ALL_WM_TAB_TRIGGERS	SELECT
PUBLIC	WMSYS	ALL_WM_VERSIONED_TABLES	SELECT
PUBLIC	WMSYS	ALL_WM_VT_ERRORS	SELECT

Question 3

Expliquer l'intéret de créer un rôle et d'attribuer les droits associés à ce rôle à un ensemble d'usagers.

Commentez la séquence suivante
create role distribue;
grant create session, select any dictionary to distribue;
grant create synonym to distribue;
grant create public database link to distribue;
grant drop public database link to distribue;
grant distribue to public;

Permet de donner le droit de relier des instances à un utilisateur.

Question 4

```
select sys_context('userenv', 'isdba') isdba from dual;

ISDBA
------------------------
FALSE
```

Return true/false si l'utilisateur courant a les droits DBA.

Question 5

```
CREATE or REPLACE FUNCTION set_md5(v_in VARCHAR2)
RETURN VARCHAR2
IS
result VARCHAR2(40);
BEGIN
1M2 2015-2016
result := UTL_RAW.CAST_TO_RAW(dbms_obfuscation_toolkit.md5(input_string=>v_in));
RETURN result;
END;
/
```