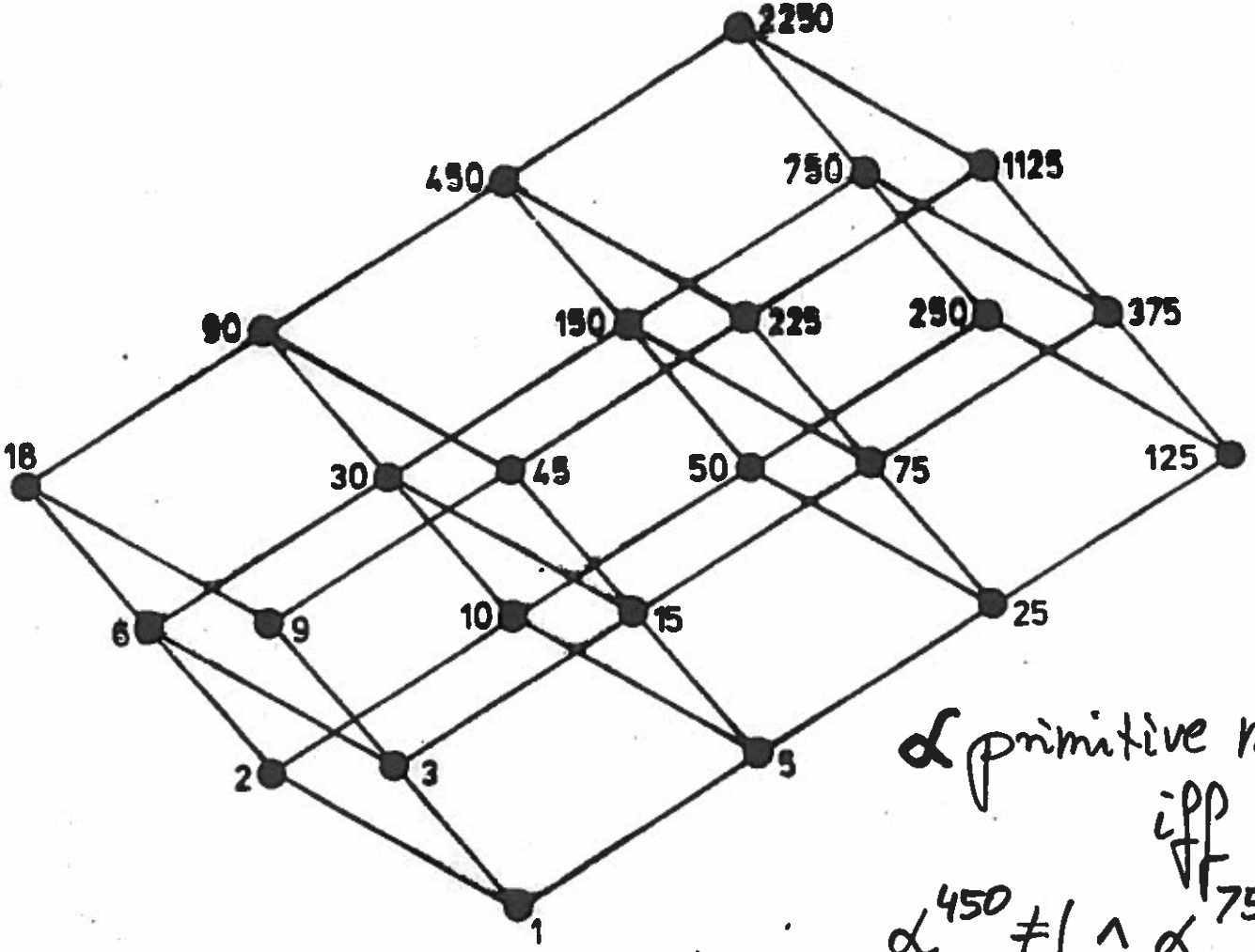
THEOREM 5.8 *Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p^*$. Then α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes q such that $q \mid (p-1)$.*

PROOF If α is a primitive element modulo p, then $\alpha^i \not\equiv 1 \pmod{p}$ for all i such that $1 \leq i \leq p-2$, so the result follows.

Conversely, suppose that $\alpha \in \mathbb{Z}_p^*$ is not a primitive element modulo p. Let d be the order of α. Then $d \mid (p-1)$ by Lagrange's theorem, and $d < p-1$ because α is not primitive. Then $(p-1)/d$ is an integer exceeding 1. Let q be a prime divisor of $(p-1)/d$. Then d is a divisor of the integer $(p-1)/q$. Since $\alpha^d \equiv 1 \pmod{p}$ and $d \mid (p-1)/q$, it follows that $\alpha^{(p-1)/q} \equiv 1 \pmod{p}$. ∎

$2250 = 2 \cdot 3^2 \cdot 5^3$

2251 prime



Thm 5.8 (Stinson):

α primitive mod 2251

iff

$\alpha^{450} \neq 1 \wedge \alpha^{750} \neq 1 \wedge$

$\alpha^{1125} \neq 1 \mod 2251$

Algorithm 5.4: RSA PARAMETER GENERATION

1. Generate two large primes, p and q, such that $p \neq q$
2. $n \leftarrow pq$ and $\phi(n) \leftarrow (p-1)(q-1)$
3. Choose a random b $(1 < b < \phi(n))$ such that $\gcd(b, \phi(n)) = 1$
4. $a \leftarrow b^{-1} \bmod \phi(n)$
5. The public key is (n, b) and the private key is (p, q, a).

Cryptosystem 5.1: *RSA Cryptosystem*

Let $n = pq$, where p and q are primes. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and define

$$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \pmod{\phi(n)}\}.$$

For $K = (n, p, q, a, b)$, define

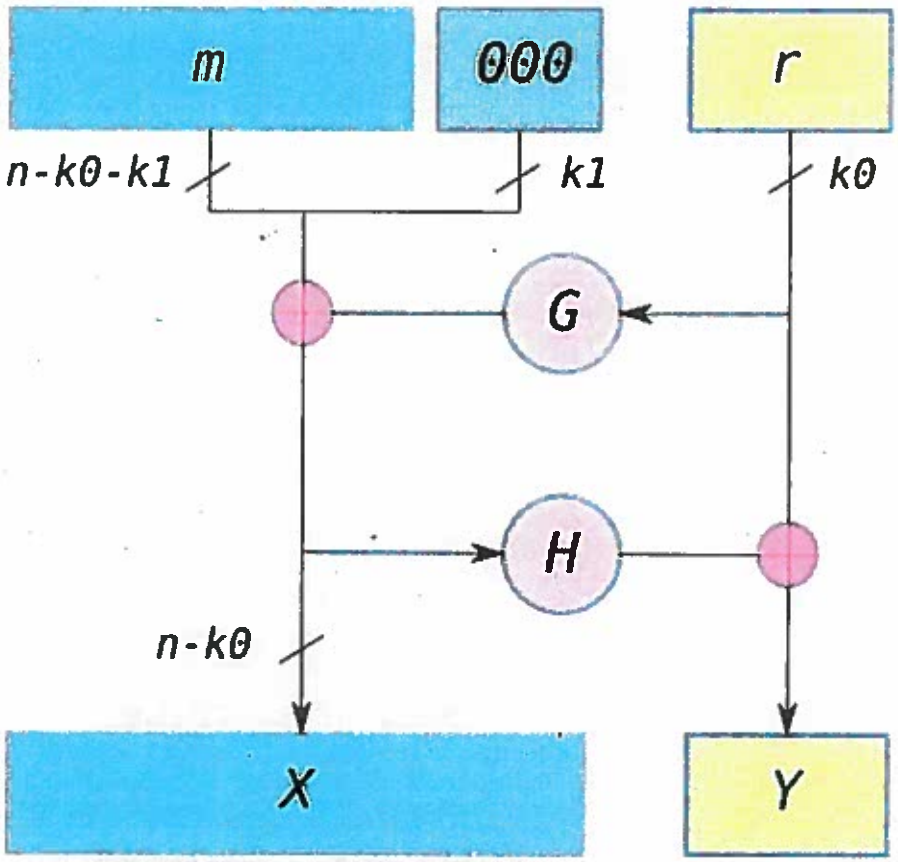
$$e_K(x) = x^b \bmod n$$

and

$$d_K(y) = y^a \bmod n$$

($x, y \in \mathbb{Z}_n$). The values n and b comprise the public key, and the values p, q and a form the private key.

OAEP padding + RSA



optimal assymetric encryption padding

Cryptosystem 5.4: *Optimal Asymmetric Encryption Padding*

Let m, k be positive integers with $m < k$, and let $k_0 = k - m$. Let $\mathcal{F}$ be a family of trapdoor one-way permutations such that $f : \{0,1\}^k \to \{0,1\}^k$ for all $f \in \mathcal{F}$. Let $G : \{0,1\}^{k_0} \to \{0,1\}^m$ and let $H : \{0,1\}^m \to \{0,1\}^{k_0}$ be "random" functions. Define $\mathcal{P} = \{0,1\}^m$, $\mathcal{C} = \{0,1\}^k$, and define

$$\mathcal{K} = \{(f, f^{-1}, G, H) : f \in \mathcal{F}\}.$$

For $K = (f, f^{-1}, G, H)$, let $r \in \{0,1\}^{k_0}$ be chosen randomly, and define

$$e_K(x) = f(y_1 \,||\, y_2),$$

where

$$y_1 = x \oplus G(r)$$

and

$$y_2 = r \oplus H(x \oplus G(r)),$$

$x, y_1 \in \{0,1\}^m$, $y_2 \in \{0,1\}^{k_0}$, and "||" denotes concatenation of vectors. Further, define

$$f^{-1}(y) = x_1 \,||\, x_2,$$

where $x_1 \in \{0,1\}^m$ and $x_2 \in \{0,1\}^{k_0}$. Then define

$$r = x_2 \oplus H(x_1)$$

and

$$d_K(y) = G(r) \oplus x_1.$$

The functions f, G and H are the public key; the function f^{-1} is the private key.

Algorithm 5.8: POLLARD $p-1$ FACTORING ALGORITHM(n, B)

$a \leftarrow 2$
for $j \leftarrow 2$ **to** B
  do $a \leftarrow a^j \bmod n$
$d \leftarrow \gcd(a-1, n)$
if $1 < d < n$
  then return (d)
  else return ("failure")

Then it must be the case that

$$(p-1) \mid B!$$

At the end of the **for** loop, we have that

$$a \equiv 2^{B!} \pmod{n}.$$

Since $p \mid n$, it must be the case that

$$a \equiv 2^{B!} \pmod{p}.$$

Now,

$$2^{p-1} \equiv 1 \pmod{p}$$

by Fermat's theorem. Since $(p-1) \mid B!$, it follows that

$$a \equiv 1 \pmod{p},$$

and hence $p \mid (a-1)$.